

Alcatel-Lucent 5620

SERVICE AWARE MANAGER | RELEASE 11.0 R8

USER GUIDE

3HE 08041 AAAH TQZZA Edition 01

Alcatel-Lucent Proprietary
This document contains proprietary information of Alcatel-Lucent and is not to be disclosed or used except in accordance with applicable agreements.
Copyright 2013-2015 © Alcatel-Lucent. All rights reserved.

Alcatel·Lucent

Alcatel-Lucent assumes no responsibility for the accuracy of the information presented, which is subject to change without notice.

Alcatel, Lucent, Alcatel-Lucent, the Alcatel-Lucent logo, lightRadio, and TiMetra are registered trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners.

Copyright 2013-2015 Alcatel-Lucent.
All rights reserved.

Disclaimers

Alcatel-Lucent products are intended for commercial uses. Without the appropriate network design engineering, they must not be sold, licensed or otherwise distributed for use in any hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life-support machines, or weapons systems, in which the failure of products could lead directly to death, personal injury, or severe physical or environmental damage. The customer hereby agrees that the use, sale, license or other distribution of the products for any such application without the prior written consent of Alcatel-Lucent, shall be at the customer's sole risk. The customer hereby agrees to defend and hold Alcatel-Lucent harmless from any claims for loss, cost, damage, expense or liability that may arise out of or in connection with the use, sale, license or other distribution of the products in such applications.

This document may contain information regarding the use and installation of non-Alcatel-Lucent products. Please note that this information is provided as a courtesy to assist you. While Alcatel-Lucent tries to ensure that this information accurately reflects information provided by the supplier, please refer to the materials provided with any non-Alcatel-Lucent product and contact the supplier for confirmation. Alcatel-Lucent assumes no responsibility or liability for incorrect or incomplete information provided about non-Alcatel-Lucent products.

However, this does not constitute a representation or warranty. The warranties provided for Alcatel-Lucent products, if any, are set forth in contractual documentation entered into by Alcatel-Lucent and its customers.

This document was originally written in English. If there is any conflict or inconsistency between the English version and any other version of a document, the English version shall prevail.

When printed by Alcatel-Lucent, this document is printed on recycled paper.

Alcatel-Lucent License Agreement

SAMPLE END USER LICENSE AGREEMENT

1. LICENSE

1.1 Subject to the terms and conditions of this Agreement, Alcatel-Lucent grants to Customer and Customer accepts a nonexclusive, nontransferable license to use any software and related documentation provided by Alcatel-Lucent pursuant to this Agreement ("Licensed Program") for Customer's own internal use, solely in conjunction with hardware supplied or approved by Alcatel-Lucent. In case of equipment failure, Customer may use the Licensed Program on a backup system, but only for such limited time as is required to rectify the failure.

1.2 Customer acknowledges that Alcatel-Lucent may have encoded within the Licensed Program optional functionality and capacity (including, but not limited to, the number of equivalent nodes, delegate workstations, paths and partitions), which may be increased upon the purchase of the applicable license extensions.

1.3 Use of the Licensed Program may be subject to the issuance of an application key, which shall be conveyed to the Customer in the form of a Supplement to this End User License Agreement. The purchase of a license extension may require the issuance of a new application key.

2. PROTECTION AND SECURITY OF LICENSED PROGRAMS

2.1 Customer acknowledges and agrees that the Licensed Program contains proprietary and confidential information of Alcatel-Lucent and its third party suppliers, and agrees to keep such information confidential. Customer shall not disclose the Licensed Program except to its employees having a need to know, and only after they have been advised of its confidential and proprietary nature and have agreed to protect same.

2.2 All rights, title and interest in and to the Licensed Program, other than those expressly granted to Customer herein, shall remain vested in Alcatel-Lucent or its third party suppliers. Customer shall not, and shall prevent others from copying, translating, modifying, creating derivative works, reverse engineering, decompiling, encumbering or otherwise using the Licensed Program except as specifically authorized under this Agreement. Notwithstanding the foregoing, Customer is authorized to make one copy for its archival purposes only. All appropriate copyright and other proprietary notices and legends shall be placed on all Licensed Programs supplied by Alcatel-Lucent, and Customer shall maintain and reproduce such notices on any full or partial copies made by it.

3. TERM

3.1 This Agreement shall become effective for each Licensed Program upon delivery of the Licensed Program to Customer.

3.2 Alcatel-Lucent may terminate this Agreement: (a) upon notice to Customer if any amount payable to Alcatel-Lucent is not paid within thirty (30) days of the date on which payment is due; (b) if Customer becomes bankrupt, makes an assignment for the benefit of its creditors, or if its assets vest or become subject to the rights of any trustee, receiver or other administrator; (c) if bankruptcy, reorganization or insolvency proceedings are instituted against Customer and not dismissed within 15 days; or (d) if Customer breaches a material provision of this Agreement and such breach is not rectified within 15 days of receipt of notice of the breach from Alcatel-Lucent.

3.3 Upon termination of this Agreement, Customer shall return or destroy all copies of the Licensed Program. All obligations of Customer arising prior to termination, and those obligations relating to confidentiality and nonuse, shall survive termination.

4. CHARGES

4.1 Upon shipment of the Licensed Program, Alcatel-Lucent will invoice Customer for all fees, and any taxes, duties and other charges. Customer will be invoiced for any license extensions upon delivery of the new software application key or, if a new application key is not required, upon delivery of the extension. All amounts shall be due and payable within thirty (30) days of receipt of invoice, and interest will be charged on any overdue amounts at the rate of 1 1/2% per month (19.6% per annum).

5. SUPPORT AND UPGRADES

5.1 Customer shall receive software support and upgrades for the Licensed Program only to the extent provided for in the applicable Alcatel-Lucent software support policy in effect from time to time, and upon payment of any applicable fees. Unless expressly excluded, this Agreement shall be deemed to apply to all updates, upgrades, revisions, enhancements and other software which may be supplied by Alcatel-Lucent to Customer from time to time.

6. WARRANTIES AND INDEMNIFICATION

6.1 Alcatel-Lucent warrants that the Licensed Program as originally delivered to Customer will function substantially in accordance with the functional description set out in the associated user documentation for a period of 90 days from the date of shipment, when used in accordance with the user documentation. Alcatel-Lucent's sole liability and Customer's sole remedy for a breach of this warranty shall be Alcatel-Lucent's good faith efforts to rectify the nonconformity or, if after repeated efforts Alcatel-Lucent is unable to rectify the nonconformity, Alcatel-Lucent shall accept return of the Licensed Program and shall refund to Customer all amounts paid in respect thereof. This warranty is available only once in respect of each Licensed Program, and is not renewed by the payment of an extension charge or upgrade fee.

6.2 ALCATEL-LUCENT EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES, REPRESENTATIONS, COVENANTS OR CONDITIONS OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, WARRANTIES OR REPRESENTATIONS OF WORKMANSHIP, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, DURABILITY, OR THAT THE OPERATION OF THE LICENSED PROGRAM WILL BE ERROR FREE OR THAT THE LICENSED PROGRAMS WILL NOT INFRINGE UPON ANY THIRD PARTY RIGHTS.

6.3 Alcatel-Lucent shall defend and indemnify Customer in any action to the extent that it is based on a claim that the Licensed Program furnished by Alcatel-Lucent infringes any patent, copyright, trade secret or other intellectual property right, provided that Customer notifies Alcatel-Lucent within ten (10) days of the existence of the claim, gives Alcatel-Lucent sole control of the litigation or settlement of the claim, and provides all such assistance as Alcatel-Lucent may reasonably require. Notwithstanding the foregoing, Alcatel-Lucent shall have no liability if the claim results from any modification or unauthorized use of the Licensed Program by Customer, and Customer shall defend and indemnify Alcatel-Lucent against any such claim.

6.4 Alcatel-Lucent Products are intended for standard commercial uses. Without the appropriate network design engineering, they must not be sold, licensed or otherwise distributed for use in any hazardous environments requiring fail safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life-support machines, or weapons systems, in which the failure of products could lead directly to death, personal injury, or severe physical or environmental damage. The Customer hereby agrees that the use, sale, license or other distribution of the Products for any such application without the prior written consent of Alcatel-Lucent, shall be at the Customer's sole risk. The Customer also agrees to defend and hold Alcatel-Lucent harmless from any claims for loss, cost, damage, expense or liability that may arise out of or in connection with the use, sale, license or other distribution of the Products in such applications.

7. LIMITATION OF LIABILITY

7.1 IN NO EVENT SHALL THE TOTAL COLLECTIVE LIABILITY OF ALCATEL-LUCENT, ITS EMPLOYEES, DIRECTORS, OFFICERS OR AGENTS FOR ANY CLAIM, REGARDLESS OF VALUE OR NATURE, EXCEED THE AMOUNT PAID UNDER THIS AGREEMENT FOR THE LICENSED PROGRAM THAT IS THE SUBJECT MATTER OF THE CLAIM. IN NO EVENT SHALL THE TOTAL COLLECTIVE LIABILITY OF ALCATEL-LUCENT, ITS EMPLOYEES, DIRECTORS, OFFICERS OR AGENTS FOR ALL CLAIMS EXCEED THE TOTAL AMOUNT PAID BY CUSTOMER TO ALCATEL-LUCENT HEREUNDER. NO PARTY SHALL BE LIABLE FOR ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES, WHETHER OR NOT SUCH DAMAGES ARE FORESEEABLE, AND/OR THE PARTY HAD BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7.2 The foregoing provision limiting the liability of Alcatel-Lucent's employees, agents, officers and directors shall be deemed to be a trust provision, and shall be enforceable by such employees, agents, officers and directors as trust beneficiaries.

8. GENERAL

8.1 Under no circumstances shall either party be liable to the other for any failure to perform its obligations (other than the payment of any monies owing) where such failure results from causes beyond that party's reasonable control.

8.2 This Agreement constitutes the entire agreement between Alcatel-Lucent and Customer and supersedes all prior oral and written communications. All amendments shall be in writing and signed by authorized representatives of both parties.

8.3 If any provision of this Agreement is held to be invalid, illegal or unenforceable, it shall be severed and the remaining provisions shall continue in full force and effect.

8.4 The Licensed Program may contain freeware or shareware obtained by Alcatel-Lucent from a third party source. No license fee has been paid by Alcatel-Lucent for the inclusion of any such freeware or shareware, and no license fee is charged to Customer for its use. The Customer agrees to be bound by any license agreement for such freeware or shareware. CUSTOMER ACKNOWLEDGES AND AGREES THAT THE THIRD PARTY SOURCE PROVIDES NO WARRANTIES AND SHALL HAVE NO LIABILITY WHATSOEVER IN RESPECT OF CUSTOMER'S POSSESSION AND/OR USE OF THE FREEWARE OR SHAREWARE.

8.5 Alcatel-Lucent shall have the right, at its own expense and upon reasonable written notice to Customer, to periodically inspect Customer's premises and such documents as it may reasonably require, for the exclusive purpose of verifying Customer's compliance with its obligations under this Agreement.

8.6 All notices shall be sent to the parties at the addresses listed above, or to any such address as may be specified from time to time. Notices shall be deemed to have been received five days after deposit with a post office when sent by registered or certified mail, postage prepaid and receipt requested.

8.7 If the Licensed Program is being acquired by or on behalf of any unit or agency of the United States Government, the following provision shall apply: If the Licensed Program is supplied to the Department of Defense, it shall be classified as "Commercial Computer Software" and the United States Government is acquiring only "restricted rights" in the Licensed Program as defined in DFARS 227-7202-1(a) and 227.7202-3(a), or equivalent. If the Licensed Program is supplied to any other unit or agency of the United States Government, rights will be defined in Clause 52.227-19 or 52.227-14 of the FAR, or if acquired by NASA, Clause 18-52.227-86(d) of the NASA Supplement to the FAR, or equivalent. If the software was acquired under a contract subject to the October 1988 Rights in Technical Data and Computer Software regulations, use, duplication and disclosure by the Government is subject to the restrictions set forth in DFARS 252-227.7013(c)(1)(ii) 1988, or equivalent.

8.8 Customer shall comply with all export regulations pertaining to the Licensed Program in effect from time to time. Without limiting the generality of the foregoing, Customer expressly warrants that it will not directly or indirectly export, reexport, or transship the Licensed Program in violation of any export laws, rules or regulations of Canada, the United States or the United Kingdom.

8.9 No term or provision of this Agreement shall be deemed waived and no breach excused unless such waiver or consent is in writing and signed by the party claimed to have waived or consented. The waiver by either party of any right hereunder, or of the failure to perform or of a breach by the other party, shall not be deemed to be a waiver of any other right hereunder or of any other breach or failure by such other party, whether of a similar nature or otherwise.

8.10 This Agreement shall be governed by and construed in accordance with the laws of the Province of Ontario. The application of the United Nations Convention on Contracts for the International Sale of Goods is hereby expressly excluded.

Preface

The Preface provides general information about the 5620 Service Aware Manager documentation suite, including this guide.

Prerequisites

Readers of the 5620 SAM documentation suite are assumed to be familiar with the following:

- 5620 SAM software structure and components
- 5620 SAM GUI operations and tools
- typical 5620 SAM management tasks and procedures
- device and network management concepts

5620 SAM documentation suite

The 5620 SAM documentation suite describes the 5620 SAM and the associated network management of its supported devices. Contact your Alcatel-Lucent support representative for information about specific network or facility considerations.

Table 1 lists the documents in the 5620 SAM customer documentation suite.

Table 1 5620 SAM customer documentation suite

Guide	Description
5620 SAM core documentation	
5620 SAM Release Description	The *5620 SAM Release Description* provides information about the new features associated with a 5620 SAM software release.

(1 of 5)

Guide	Description
5620 SAM Release Notice	The *5620 SAM Release Notice* provides important information about the software release, including outstanding issues and restrictions. This document is not shipped with the on-product customer documentation and must be obtained from OLCS as described in Documentation and resources on the web.
5620 SAM Planning Guide	The *5620 SAM Planning Guide* provides information about 5620 SAM scalability and recommended hardware configurations.
5620 SAM System Architecture Guide	The *5620 SAM System Architecture Guide* is intended for technology officers, network planners, and system administrators to increase their knowledge of the 5620 SAM software structure and components. It describes the system structure, software components, and interfaces of the 5620 SAM. In addition, 5620 SAM fault tolerance, security, and network management capabilities are discussed from an architectural perspective.
5620 SAM | 5650 CPAM Installation and Upgrade Guide	The *5620 SAM | 5650 CPAM Installation and Upgrade Guide* provides OS considerations, configuration information, and procedures for the following: • installing, upgrading, and uninstalling 5620 SAM and 5650 CPAM software in standalone and redundant deployments • 5620 SAM system migration to a different system • conversion from a standalone to a redundant 5620 SAM system
5620 SAM User Guide	The *5620 SAM User Guide* provides information about using the 5620 SAM to manage the service-aware IP/MPLS network, including GUI basics, service configuration, and policy management. The *5620 SAM User Guide* uses a task-based format that employs both high-level workflows and detailed procedures. 5620 SAM management information specific to LTE network elements is covered in the *5620 SAM LTE EPC User Guide* and *5620 SAM LTE RAN User Guide*. 5620 SAM management information specific to 1830 PSS network elements is covered in the *5620 SAM Optical User Guide*.
5620 SAM System Administrator Guide	The *5620 SAM System Administrator Guide* provides information about the tasks performed by a user with a 5620 SAM admin role, including: • 5620 SAM security management tasks such as setting up all required user accounts and user groups • advanced configuration tasks such as configuring, maintaining, and administering the 5620 SAM operational environment • routine maintenance tasks to maintain the 5620 SAM hardware and system integrity and efficiencies
5620 SAM Integration Guide	The *5620 SAM Integration Guide* provides procedures to allow the 5620 SAM to integrate with other Alcatel-Lucent products and third-party products.
5620 SAM Supervision Module User Guide	The *5620 SAM Supervision Module User Guide* provides information about how to configure and use the web-based 5620 SAM Supervision Module for fault management and at-a-glance network element monitoring.
5620 SAM Scripts and Templates Developer Guide	The *5620 SAM Scripts and Templates Developer Guide* provides information that allows users to develop, manage, and run CLI-based or XML-based scripts or templates. The guide is intended for developers, skilled administrators, and operators who are expected to be familiar with the following: • CLI scripting, XML, and the Velocity engine • basic scripting or programming • 5620 SAM functions

(2 of 5)

Guide	Description
5620 SAM Parameter Guide	The *5620 SAM Parameter Guide* provides: • parameter descriptions that include value ranges and default values • parameter options and option descriptions • parameter and option dependencies • parameter mappings to the 5620 SAM-O XML equivalent property names Parameters specific to LTE network elements are covered in the *5620 SAM LTE Parameter Reference*. Parameters specific to 1830 PSS network elements are covered in the *5620 SAM Optical Parameter Reference*. The 5620 SAM online help system includes a Parameter Search Tool that allows you to look up parameters or 5620 SAM and 5650 CPAM forms. See the *5620 SAM User Guide* for more information about using the Parameter Search Tool.
5620 SAM Statistics Management Guide	The *5620 SAM Statistics Management Guide* provides information about how to configure performance and accounting statistics collection and how to view counters using the 5620 SAM. Network examples are included.

5620 SAM Troubleshooting Guide	The *5620 SAM Troubleshooting Guide* provides task-based procedures and user documentation to:
	• help resolve issues in the managed and management networks
	• identify the root cause and plan corrective action for:
	  • alarm conditions on a network object or customer service
	  • problems on customer services with no associated alarms
	• list problem scenarios, possible solutions, and tools to help check:
	  • network management LANs
	  • network management platforms and operating systems
	  • 5620 SAM client GUIs and client OSS applications
	  • 5620 SAM servers
	  • 5620 SAM databases

5620 SAM Alarm Reference	The *5620 SAM Alarm Reference* provides a description of all alarms supported on the 5620 SAM, including LTE and optical alarms, the raising and clearing conditions of each alarm, and the remedial action to fix the problem. The reference is organized by network element type.
5620 SAM Glossary	The *5620 SAM Glossary* defines terms and acronyms used in all of the 5620 SAM documentation, including 5620 SAM LTE documentation.
5620 SAM Network Element Compatibility Guide	The *5620 SAM Network Element Compatibility Guide* provides release-specific information about the compatibility of managed devices in 5620 SAM releases. This document is updated regularly; always consult the latest version on OLCS as described in Documentation and resources on the web.
5620 SAM MPR documentation	
5620 SAM MPR User Guide	The *5620 SAM MPR User Guide* describes how to discover, configure, and manage 9500 MPR and 9500 MPRe devices using the 5620 SAM. The guide is intended for network planners, administrators, and operators and is to be used in conjunction with other guides in the 5620 SAM documentation suite where management of 9500 MPR and 9500 MPRe devices does not differ from other network elements. Alcatel-Lucent recommends that you review the entire *5620 SAM MPR User Guide* before you attempt to use the 5620 SAM in your MPR network.
5620 SAM LTE documentation	
5620 SAM LTE Release Description	The *5620 SAM LTE Release Description* provides information about the LTE features associated with the release.

(3 of 5)

Guide	Description
5620 SAM LTE EPC User Guide	The *5620 SAM LTE EPC User Guide* describes how to discover, configure, and manage LTE ePC devices using the 5620 SAM. The guide is intended for LTE ePC network planners, administrators, and operators and is to be used in conjunction with other guides in the 5620 SAM documentation suite where management of ePC devices does not differ from other network elements. Alcatel-Lucent recommends that you review the entire *5620 SAM LTE EPC User Guide* before you attempt to use the 5620 SAM in your LTE network.
5620 SAM LTE RAN User Guide	The *5620 SAM LTE RAN User Guide* describes how to discover, configure, and manage the Evolved NodeB, or eNodeB, using the 5620 SAM. The guide is intended for LTE RAN network planners, administrators, and operators and is to be used in conjunction with other guides in the 5620 SAM documentation suite where management of RAN devices does not differ from other network elements. Alcatel-Lucent recommends that you review the entire *5620 SAM LTE RAN User Guide* before you attempt to use the 5620 SAM in your LTE network.
5620 SAM LTE Parameter Reference	The *5620 SAM LTE Parameter Reference* provides a list of all LTE ePC and LTE RAN parameters supported in the 5620 SAM.
5620 SAM LTE OSS Interface Developer Guide	The *5620 SAM LTE OSS Interface Developer Guide* provides information about developing LTE OSS applications, including information about the 3GPP OSS interface components and architecture, understanding the 5620 SAM-O schema in the context of LTE, compliance with 3GPP standards, and typical operational scenarios.
5620 SAM optical documentation	
5620 SAM Optical User Guide	The *5620 SAM Optical User Guide* describes how to discover, configure, and manage optical devices using the 5620 SAM. The guide is intended for optical network planners, administrators, and operators and is to be used in conjunction with other guides in the 5620 SAM documentation suite where management of optical devices does not differ from other network elements. Alcatel-Lucent recommends that you review the entire *5620 SAM Optical User Guide* before you attempt to use the 5620 SAM in your optical network.
5620 SAM Optical Parameter Reference	The *5620 SAM Optical Parameter Reference* provides a list of all optical device parameters supported in the 5620 SAM.
5620 SAM-O documentation	
5620 SAM XML OSS Interface Developer Guide	The *5620 SAM XML OSS Interface Developer Guide* provides information that allows you to: • use the 5620 SAM XML OSS interface to access network management information • learn about the information model associated with the managed network • develop OSS applications using the packaged methods, classes, data types, and objects necessary to manage 5620 SAM functions
5650 CPAM documentation	
5650 CPAM Release Description	The *5650 CPAM Release Description* provides information about the new features associated with a 5650 CPAM software release.
5650 CPAM Release Notice	The *5650 CPAM Release Notice* provides important information about the 5650 CPAM software release and corresponding 7701 CPAA software release, including outstanding issues and restrictions. This document is not shipped with the on-product documentation and must be obtained from OLCS as described in Documentation and resources on the web.
5650 CPAM User Guide	The *5650 CPAM User Guide* describes how to capture, inspect, visualize, and troubleshoot IGP and BGP topologies using the 5650 CPAM.
7701 CPAA Hardware Revision 1 Setup and Software Installation Instructions	The *7701 CPAA Hardware Revision 1 Setup and Software Installation Instructions* describes the hardware setup and software installation for the 7701 CPAA Hardware Revision 1, the route analyzer component of the 5650 CPAM.

(4 of 5)

Guide	Description
7701 CPAA Hardware Revision 2 Setup and Software Installation Instructions	The *7701 CPAA Hardware Revision 2 Setup and Software Installation Instructions* describes the hardware setup and software installation for the 7701 CPAA Hardware Revision 2, the route analyzer component of the 5650 CPAM.

(5 of 5)

Obtaining customer documentation

You can obtain 5620 SAM customer documentation:

- from the product
- on the web

On-product documentation

The 5620 SAM on-product customer documentation is delivered in HTML and PDF. Choose Help→User Documentation from the 5620 SAM client GUI to open the help system in a web browser. For best results, use Internet Explorer or Firefox.

The help system opens to the User Documentation Index, which provides a summary of and links to all 5620 SAM customer documents.

Click on the Using the help system tab on the User Documentation Index page to find usage tips for navigating and searching within the on-product customer documentation.

You can return to the User Documentation Index at any time by clicking on the Home icon, shown in Figure 1.

Figure 1 Home icon



Documentation and resources on the web

The 5620 SAM customer documentation is available for download in PDF format from the Alcatel-Lucent Customer Support Center: http://www.alcatel-lucent.com/myaccess. If you are a new user and require access to this service, please contact your Alcatel-Lucent support representative.

Release Notices and any other documents not delivered on-product are posted to this site.

5620 SAM product alerts

Product technical alerts are used to communicate important information to customers about released loads. You can view and subscribe to product alerts for the 5620 SAM from the Alcatel-Lucent Customer Support Center.

Working with PDFs

You can download PDFs of individual guides from the Alcatel-Lucent Customer Support Center, or you can choose to download a zip of all PDFs for a particular release.

You can use the Search function of Acrobat Reader (File→Search) to find a term in a PDF of any 5620 SAM document. To refine your search, use appropriate search options (for example, search for whole words only or enable case-sensitive searching). You can also search for a term in multiple PDFs at once, provided that they are located in the same directory. For more information, see the Help for Acrobat Reader.



Note — Users of Mozilla browsers may receive an error message when opening the PDF files in the 5620 SAM documentation suite. The offline storage and default cache values used by the browsers are the cause of the error message.

Alcatel-Lucent recommends changing the Mozilla Firefox offline storage or Mozilla 1.7 cache value to 100 Mbytes to eliminate the error message.

Documentation conventions

Table 2 lists the conventions that are used throughout the documentation.

Table 2 Documentation conventions

Convention	Description	Example
Key name	Press a keyboard key	Delete
Italics	Identifies a variable	*hostname*
Key+Key	Type the appropriate consecutive keystroke sequence	CTRL+G
Key-Key	Type the appropriate simultaneous keystroke sequence	CTRL-G
*	An asterisk is a wildcard character, which means “any character” in a search argument.	log_file*.txt
↵	Press the Return key	↵
—	An em dash indicates there is no information.	—
→	Indicates that a cascading submenu results from selecting a menu item	Policies→Alarm Policies

Procedures with options or substeps

When there are options in a procedure, they are identified by letters. When there are substeps in a procedure, they are identified by Roman numerals.

Example of options in a procedure

At step 1, you can choose option a or b. At step 2, you must do what the step indicates.

1 This step offers two options. You must choose one of the following.

   a This is one option.

   b This is another option.

2 You must perform this step.

Example of substeps in a procedure

At step 1, you must perform a series of substeps within a step. At step 2, you must do what the step indicates.

1 This step has a series of substeps that you must perform to complete the step. You must perform the following substeps.

   i This is the first substep.

   ii This is the second substep.

   iii This is the third substep.

2 You must perform this step.

Measurement conventions

Measurements in this document are expressed in metric units and follow the Système international d'unités (SI) standard for abbreviation of metric units. If imperial measurements are included, they appear in brackets following the metric unit.

Table 3 lists the measurement symbols used in this document.

Table 3 Bits and bytes conventions

Measurement	Symbol
bit	b
byte	byte
kilobits per second	kb/s

Important information

The following conventions are used to indicate important information:



Warning — Warning indicates that the described activity or situation may, or will, cause equipment damage or serious performance problems.



Caution — Caution indicates that the described activity or situation may, or will, cause service interruption.



Note — Notes provide information that is, or may be, of special interest.

Contents

Preface **ix**

Prerequisites ix
5620 SAM documentation suite ix
Obtaining customer documentation xiii
On-product documentation xiii
Documentation and resources on the web xiii
Documentation conventions xiv
Procedures with options or substeps xiv
Measurement conventions xv
Important information xvi

Getting started

1 — What's new? 1-1

1.1 What's new in 5620 SAM Release 11.0 1-2
What's new in 5620 SAM Release 11.0 R8 1-2
What's new in 5620 SAM Release 11.0 R7 1-2
What's new in 5620 SAM Release 11.0 R6 1-5
What's new in 5620 SAM Release 11.0 R5 1-5
What's new in 5620 SAM Release 11.0 R4 1-19
What's new in 5620 SAM Release 11.0 R3 1-19
What's new in 5620 SAM Release 11.0 R2 1-24
What's new in 5620 SAM Release 11.0 R1 1-24

2 — 5620 SAM system overview 2-1

2.1 5620 SAM system overview 2-2
5620 SAM system architecture 2-2
Supported network management modules 2-3
2.2 About this guide 2-3

3 — 5620 SAM GUI overview 3-1

3.1 5620 SAM GUI overview 3-2
Custom workspaces 3-3
Shortcut keys 3-4
Windows and forms 3-4
Multi-edit property forms 3-4
5620 SAM clipboard 3-5
Floating windows 3-5
User preferences 3-6
System preferences 3-6
External windows 3-7
Navigation tree 3-7
Contextual menus 3-7
Indicators and icons 3-7
Task manager 3-8
Text message 3-9
Maps 3-9
Alarm Window 3-9
Forms 3-9
Parameter Search Tool 3-15
Localized language support 3-16
3.2 Using search functions 3-16
Using search filters 3-17
Searches using Boolean operators 3-18
Invalid attributes or values 3-19
Preset filters 3-19
Span of control filters 3-20
Equipment group filters 3-20
Locating attributes on configuration forms 3-20
3.3 Workflow to use the 5620 SAM GUI 3-21
3.4 5620 SAM GUI opening and closing procedures 3-21
Procedure 3-1 To open a single-user GUI client on a Windows station 3-22
Procedure 3-2 To open a single-user GUI client on a RHEL or Solaris station 3-26
Procedure 3-3 To open a client GUI through a client delegate server 3-29
Procedure 3-4 To change to a different 5620 SAM client GUI user 3-30
Procedure 3-5 To close the 5620 SAM GUI 3-30
3.5 Basic 5620 SAM GUI operation procedures 3-31
Procedure 3-6 To open or close a main window 3-31
Procedure 3-7 To close one or all open forms 3-32
Procedure 3-8 To show or hide a window or form 3-32
Procedure 3-9 To arrange windows and forms 3-33
Procedure 3-10 To move a window or form to an external window 3-34
Procedure 3-11 To send a text message to other 5620 SAM users 3-34

Procedure 3-12 To use menus, the toolbar, or shortcuts 3-35
Procedure 3-13 To use menus, windows, and forms to configure or view parameters 3-35
Procedure 3-14 To use the Parameter Search Tool 3-37
Procedure 3-15 To use the 5620 SAM clipboard 3-39
Procedure 3-16 To copy a property form to the clipboard 3-39
Procedure 3-17 To open a property form copied to the clipboard 3-40
Procedure 3-18 To open property forms from the clipboard menu 3-40
3.6 5620 SAM GUI user preferences configuration procedures 3-40
Procedure 3-19 To configure 5620 SAM user preferences 3-40
Procedure 3-20 To customize tabs on configuration forms 3-42
Procedure 3-21 To temporarily display hidden tabs on configuration forms 3-44
Procedure 3-22 To configure the current client time zone 3-44
3.7 5620 SAM GUI search procedures 3-45
Procedure 3-23 To monitor the 5620 SAM Task Manager 3-45
Procedure 3-24 To perform a simple search using column headings 3-46
Procedure 3-25 To perform an advanced search 3-47
Procedure 3-26 To perform a search by specifying endpoints 3-49
Procedure 3-27 To locate an attribute on a configuration form 3-50
Procedure 3-28 To filter object types 3-51
Procedure 3-29 To filter using span of control 3-51
Procedure 3-30 To view and manage listed information 3-52
Procedure 3-31 To save listed information to a file 3-57
Procedure 3-32 To save results list preferences 3-58
Procedure 3-33 To save search filters 3-58
Procedure 3-34 To clear a search filter 3-59
Procedure 3-35 To load a saved search filter 3-60
Procedure 3-36 To delete a saved search filter 3-61
Procedure 3-37 To configure equipment group search filters 3-61
Procedure 3-38 To perform a search using equipment group filters 3-63

4 — 5620 SAM custom workspaces 4-1

4.1 5620 SAM custom workspaces overview 4-2
Workspace customization 4-2
5620 SAM upgrades and custom workspace updates 4-2
Custom tab display 4-3
4.2 Workflow to administer 5620 SAM custom workspaces 4-3
4.3 Workflow to customize 5620 SAM workspaces 4-3
4.4 Workflow to save and update custom workspaces for a 5620 SAM upgrade 4-4
4.5 5620 SAM GUI custom workspace procedures 4-4
Procedure 4-1 To customize menus 4-4
Procedure 4-2 To customize toolbars 4-7
Procedure 4-3 To customize tree labels 4-9
Procedure 4-4 To customize topology map icon labels 4-10
Procedure 4-5 To customize window layouts 4-10
Procedure 4-6 To add or remove a workspace in the workspace selector 4-11
Procedure 4-7 To change to another workspace using the workspace selector 4-12

Procedure 4-8 To delete a workspace from the 5620 SAM 4-12
Procedure 4-9 To export custom workspaces 4-13
Procedure 4-10 To import a workspace 4-13
Procedure 4-11 To add new menu items to a saved custom workspace after a 5620 SAM upgrade 4-14

5 — 5620 SAM navigation tree overview 5-1
5.1 Navigation tree overview 5-2
Using the navigation tree toolbar 5-4
Contextual menus 5-6
5.2 Basic navigation tree procedures 5-11
Procedure 5-1 To search for objects in the navigation tree 5-12
Procedure 5-2 To make a selected object the root of the navigation tree 5-13
Procedure 5-3 To make a selected object the root of another navigation tree 5-13
Procedure 5-4 To restore the default navigation tree root 5-13

6 — 5620 SAM topology map management 6-1
6.1 5620 SAM topology map management overview 6-2
Map window 6-2
Map panel 6-3
Map navigation tree 6-5
Map toolbar 6-6
Zooming in and out 6-11
Bookmarks 6-11
Information tables 6-13
6.2 5620 SAM topology map types 6-14
Physical topology map 6-14
Service tunnel topology map 6-16
EPS path topology maps 6-17
LSP path topology map 6-17
LSP cross-connect topology map 6-18
Flat maps 6-18
Service topology maps 6-19
Composite service topology maps 6-22
6.3 Working with topology maps 6-23
Modifying a service from the topology view 6-24
Managing OAM diagnostics from the topology view 6-24
6.4 Workflow to use 5620 SAM topology maps 6-26
6.5 Basic 5620 SAM topology map procedures 6-27
Procedure 6-1 To open a map from the 5620 SAM main menu 6-27
Procedure 6-2 To open a service topology map 6-27
Procedure 6-3 To open an MPLS provisioned path map from the MPLS Path form 6-27
Procedure 6-4 To open a dynamic LSP path map from the LSP Path form 6-28
Procedure 6-5 To open a flat map 6-29
Procedure 6-6 To open a dynamic LSP cross-connect topology map 6-29
Procedure 6-7 To view and understand map elements 6-30

Procedure 6-8 To save a map to a file 6-31
Procedure 6-9 To view object information from a map 6-32
Procedure 6-10 To manage the topology map window 6-32
Procedure 6-11 To zoom in and zoom out on a map 6-33
Procedure 6-12 To display only selected map objects 6-33
Procedure 6-13 To display only highlighted map objects 6-34
6.6 5620 SAM topology map configuration procedures 6-34
Procedure 6-14 To create an information table configuration 6-34
Procedure 6-15 To enable or disable a global information table 6-35
Procedure 6-16 To enable or disable a selected information table 6-36
Procedure 6-17 To re-enable or disable map highlights 6-36
Procedure 6-18 To enable or disable a highlight information table 6-37
Procedure 6-19 To delete a map highlight 6-37
Procedure 6-20 To create a map filter 6-38
Procedure 6-21 To load and apply a saved filter to a topology map 6-39
Procedure 6-22 To auto-layout icons on a map 6-40
Procedure 6-23 To search for a specific network object 6-41
Procedure 6-24 To create a bookmark 6-42
Procedure 6-25 To manage bookmarks 6-43
Procedure 6-26 To change the map background image 6-44
6.7 5620 SAM topology map management procedures 6-44
Procedure 6-27 To use OAM diagnostic functions on service topology and composite service flat topology maps 6-45
Procedure 6-28 To create a topology group 6-46
Procedure 6-29 To populate a topology group 6-47
Procedure 6-30 To modify a topology group and create topology groups with the same parameter settings 6-47
Procedure 6-31 To delete a topology group 6-48
Procedure 6-32 To modify a service or composite service using the topology view 6-48
Procedure 6-33 To create a physical link 6-49
Procedure 6-34 To modify a physical link and create physical links with the same parameter settings 6-54
Procedure 6-35 To manage link referencing 6-55
Procedure 6-36 To delete a physical link 6-55
Procedure 6-37 To configure bandwidth availability on physical links 6-56
Procedure 6-38 To view and modify discovered physical link properties 6-57
Procedure 6-39 To switch from a backup/standby protected link to an in-service protected link on a 9500 MPR device 6-58

7 — 5620 SAM scheduling 7-1

7.1 Scheduling overview 7-2
SAM schedules 7-3
7.2 Workflow to manage scheduling 7-4
7.3 Scheduling procedures 7-5
Procedure 7-1 To configure a SAM schedule 7-5
Procedure 7-2 To associate a task with a 5620 SAM schedule 7-7
Procedure 7-3 To modify a scheduled task 7-8

Procedure 7-4 To assign a different user account to a SAM scheduled task 7-9
Procedure 7-5 To turn up or shut down a scheduled task..... 7-9
Procedure 7-6 To view the current status of a SAM scheduled task..... 7-10
Procedure 7-7 To execute a SAM scheduled task..... 7-10
Procedure 7-8 To reset a scheduled task..... 7-11
Procedure 7-9 To delete a scheduled task 7-11
Procedure 7-10 To delete a schedule 7-12

Device management

8 — Device support 8-1

8.1 Device support overview 8-3
Device-specific workflows 8-4
8.2 Workflow to prepare 5620 SAM to manage devices 8-4
8.3 1830 PSS support 8-6
8.4 5780 DSC support 8-6
8.5 7210 SAS support 8-6
7210 SAS-D support 8-7
7210 SAS-E support 8-7
7210 SAS-M and 7210 SAS-X support 8-7
7210 SAS-T support 8-8
System resource profile 8-8
8.6 Workflow to manage 7210 SAS devices 8-10
8.7 7450 ESS support 8-13
8.8 Workflow to manage 7450 ESS devices 8-13
8.9 7705 SAR support 8-16
7705 SAR MWA support 8-16
7705 SAR NEtO support 8-17
7705 SAR auxiliary alarm daughter cards 8-17
7705 SAR 6-port E&M daughter cards 8-17
7705 SAR 12-port SDI card 8-18
7705 SAR Power Injector card 8-18
7705 SAR Optical Add/Drop Mux cards 8-18
7705 SAR CSMv2 card 8-18
7705 SAR 2 × 10-Gig Bridged Ethernet XFP + 1 × 2.5G Virtual Ethernet card 8-18
7705 SAR 6-port FXS Adapter card 8-19
7705 SAR 8-port FXO Adapter card 8-19
7705 SAR 10-port 1GigE/1-port 10GigE X-Adapter card 8-19
7705 SAR 8-port GigE SFP card (-48/+24 VDC) 8-20
7705 SAR Packet Microwave card 8-20
7705 SAR Voice & Tele-Protection MDA 8-20
7705 SAR-A 8-20
7705 SAR-F 8-20
7705 SAR-H 8-21
7705 SAR-M 8-21
7705 SAR-W 8-22

8.10 Workflow to manage 7705 SAR devices 8-22
8.11 7710 SR support 8-25
8.12 Workflow to manage 7710 SR devices 8-25
8.13 7750 MG support 8-28
8.14 7750 SR support 8-28
7750 SR-c4 8-28
7750 SR-c12 8-29
7750 SR-12E 8-29
8.15 Workflow to manage 7750 SR devices 8-29
8.16 7950 XRS support 8-32
Variants 8-32
Shelf components 8-33
8.17 Workflow to manage 7950 XRS devices 8-34
8.18 9471 WMM support 8-37
8.19 9500 MPR and 9500 MPRe support 8-37
8.20 eNodeB support 8-38
8.21 OmniSwitch support 8-38
OmniSwitch LAG objects 8-42
Using WebView to manage an OmniSwitch 8-42
8.22 Workflow to manage OmniSwitch devices 8-43
8.23 GNE support 8-46
Statistics support 8-47
Alarm support 8-48
8.24 Workflow to manage GNEs 8-49

9 — Device commissioning and management 9-1

9.1 Device commissioning overview 9-2
In-band and out-of-band management 9-2
IPv6 device management 9-6
Secure file transfers 9-6
9.2 GNE commissioning overview 9-6
Using alternate element managers 9-7
GNE profiles 9-7
Configuring user-defined alarms for GNEs 9-8
9.3 Workflow to commission Alcatel-Lucent devices 9-9
9.4 Device commissioning procedures 9-10
Procedure 9-1 To commission a device for 5620 SAM management 9-11
Procedure 9-2 To commission an OmniSwitch for 5620 SAM management 9-14
Procedure 9-3 To configure the 5620 SAM SNMP trap sources 9-18
Procedure 9-4 To configure polling for a 7450 ESS, 7705 SAR, 7710 SR, 7750 SR, or 7950 XRS 9-20
Procedure 9-5 To configure polling for a 7210 SAS 9-21
Procedure 9-6 To edit polling settings for multiple devices 9-24
9.5 Workflow to commission GNEs 9-24
9.6 GNE commissioning procedures 9-25
Procedure 9-7 To prepare a GNE for 5620 SAM management 9-25
Procedure 9-8 To configure an alternate EMS for a specific GNE 9-28
Procedure 9-9 To prepare a 9400 AWY or 9500 MSS-1c for 5620 SAM management 9-29
Procedure 9-10 To modify a GNE profile 9-31

Procedure 9-11 To delete a GNE profile 9-32
Procedure 9-12 To create a GNE alarm catalog 9-33
Procedure 9-13 To create a transform function for a GNE alarm catalog 9-37
Procedure 9-14 To add an alarm mapping to a GNE alarm catalog 9-38
Procedure 9-15 To modify or delete a GNE alarm mapping 9-39
Procedure 9-16 To delete a GNE alarm catalog 9-40
Procedure 9-17 To cross launch the 9400 AWY or 9500 MSS-1c J-USM manager 9-42

10 — Device discovery 10-1

10.1 Device discovery overview 10-2
Suspending device management 10-2
Unmanaging and deleting devices 10-4
Post-discovery actions 10-4
SNMP management 10-5
IPv6 discovery 10-6
Discovery and SNMP packet size 10-6
9500 MPR radio link discovery and management 10-7
10.2 Resynchronization of NEs 10-8
10.3 Mediation and SNMP MIBs 10-9
10.4 SSH security 10-9
SSH2 host key management 10-10
SSH2 and device CLI sessions 10-10
SSH2 and script management 10-10
SSH2 and secure file transfers 10-10
10.5 Server resource management 10-11
10.6 SNMP event notification policies 10-11
10.7 Workflow to discover network devices 10-12
10.8 Device discovery procedures 10-14
Procedure 10-1 To configure SNMPv3 on a device 10-14
Procedure 10-2 To verify that SSH2 is enabled on a device 10-18
Procedure 10-3 To enable SSH host key persistence on a device 10-19
Procedure 10-4 To configure NE mediation 10-19
Procedure 10-5 To configure a post-discovery action 10-24
Procedure 10-6 To configure a discovery rule 10-24
Procedure 10-7 To discover devices 10-29
Procedure 10-8 To view the post-discovery action execution status 10-31
Procedure 10-9 To manage a post-discovery action failure on an NE 10-32
Procedure 10-10 To configure an event notification policy 10-33
Procedure 10-11 To assign an event notification policy to an NE 10-35
Procedure 10-12 To edit a discovery rule 10-36
Procedure 10-13 To enable or disable a discovery rule 10-37
Procedure 10-14 To delete a discovery rule 10-37
Procedure 10-15 To rescan the network according to a discovery rule 10-37
Procedure 10-16 To manage, suspend, or unmanage a device 10-38
Procedure 10-17 To specify which management address the 5620 SAM uses to remanage a device 10-39
Procedure 10-18 To delete a device 10-39

Procedure 10-19 To partially or fully resynchronize NEs with the 5620 SAM database 10-40
Procedure 10-20 To list the active and mismatched SSH host keys 10-41
Procedure 10-21 To manually accept a mismatched SSH host key 10-42
Procedure 10-22 To change from SNMPv2c to SNMPv3 management of a device 10-43
Procedure 10-23 To switch from non-secure to secure mediation 10-43
Procedure 10-24 To list and save SNMP MIB information 10-45

11 — Device CLI sessions 11-1

11.1 Device CLI sessions overview 11-2
vi editor support 11-2
11.2 Workflow to use a 5620 SAM CLI 11-3
11.3 CLI procedures 11-3
Procedure 11-1 To configure the 5620 SAM CLI console preferences 11-3
Procedure 11-2 To open and close a 5620 SAM device CLI session 11-4

12 — Working with network objects 12-1

12.1 Working with network objects overview 12-2
Object deployment status 12-3
12.2 Working with topology group objects 12-3
12.3 Working with physical links 12-4
12.4 Workflow to manage network objects 12-5
12.5 Working with network objects procedures 12-5
Procedure 12-1 To monitor the deployment status of a network object 12-5

13 — Device object configuration 13-1

13.1 Device object configuration overview 13-2
13.2 Working with device objects 13-2
13.3 Working with ring group objects 13-2
13.4 Workflow to manage device objects 13-3
13.5 General device configuration procedures 13-5
Procedure 13-1 To create an object 13-5
Procedure 13-2 To modify NE properties 13-5
Procedure 13-3 To configure custom NE property values in the NE form 13-5
Procedure 13-4 To create an operational group 13-6
Procedure 13-5 To enable and configure global cflowd on an NE 13-7
Procedure 13-6 To add a span of control to an NE 13-8
Procedure 13-7 To configure load balancing 13-8
Procedure 13-8 To enable or disable 802.1X 13-9
Procedure 13-9 To configure exclusive policy editing on an NE 13-10
Procedure 13-10 To configure active card alarms on an NE 13-11
Procedure 13-11 To configure a TWAMP server 13-11
Procedure 13-12 To enable LLDP on an NE 13-14
Procedure 13-13 To configure the BFD flap detection interval on an NE 13-15
Procedure 13-14 To configure an IP next hop limit on an NE 13-15

Procedure 13-15 To create a chassis-level PBB configuration 13-15
Procedure 13-16 To configure serving network information on an NE ... 13-16
Procedure 13-17 To configure the RADIUS CoA port on an NE 13-16
Procedure 13-18 To configure two WRED slopes on a 7210 SAS 13-17
Procedure 13-19 To enable frame-based accounting for QoS policies ... 13-18
Procedure 13-20 To configure the system resource profile on a 7210 SAS 13-18
Procedure 13-21 To enable or disable ICMP extensions 13-21
Procedure 13-22 To configure subscriber data persistence 13-21
Procedure 13-23 To configure QoS ingress aggregate rates on the 7705 SAR-M/ME 13-22
Procedure 13-24 To launch an MCT on a 9500 MPRe NE connected to a 7705 SAR 13-22
Procedure 13-25 To start and stop a Webview or Secure Webview session on an OmniSwitch 13-23
Procedure 13-26 To configure the dying gasp alarm on an OS 6250M NE 13-24
13.6 Ring group configuration procedures 13-24
Procedure 13-27 To create a ring group 13-24
Procedure 13-28 To remove a ring group or ring group device 13-26

14 — Logical group object configuration 14-1

14.1 Logical group object configuration overview 14-2
14.2 Working with CCAG objects 14-2
14.3 Working with ISA-AA groups 14-2
14.4 Working with ISA-Tunnel groups 14-3
14.5 Working with ISA-LNS groups 14-4
14.6 Working with ISA-NAT groups 14-4
14.7 Working with ISA-Video groups 14-4
14.8 Working with ISA-WLAN GW groups 14-5
Soft GRE tunnels 14-5
14.9 Working with IGH objects 14-6
14.10 Working with LAG objects 14-6
LAG link mapping profiles 14-7
LAG utilization TCAs 14-7
BFD on Ethernet LAGs 14-8
14.11 Workflow to manage logical group objects 14-8
14.12 Logical group object configuration procedures 14-9
Procedure 14-1 To configure a CCAG 14-9
Procedure 14-2 To configure an ISA-AA group and ISA-AA partitions 14-11
Procedure 14-3 To add an AA subscriber policy override to an ISA-AA group or partition 14-18
Procedure 14-4 To configure cflowd on an ISA-AA group or partition 14-20
Procedure 14-5 To configure an ISA-tunnel group 14-22
Procedure 14-6 To configure an ISA-LNS group 14-23
Procedure 14-7 To configure an ISA-Video group 14-24
Procedure 14-8 To configure an ISA-WLAN GW group 14-25
Procedure 14-9 To create an IGH and add members 14-26
14.13 LAG configuration procedures 14-27
Procedure 14-10 To create a LAG 14-27
Procedure 14-11 To configure a LAG 14-32

Procedure 14-12 To configure an OmniSwitch LAG 14-36
Procedure 14-13 To configure OmniSwitch dynamic LAG members 14-40
Procedure 14-14 To create a LAG link mapping profile 14-42
Procedure 14-15 To configure BFD on a LAG 14-44
Procedure 14-16 To view micro-BFD sessions on a LAG 14-44

15 — Shelf object configuration 15-1

15.1 Shelf object configuration overview 15-2
15.2 Working with shelf objects 15-2
Chassis modes 15-2
Timing synchronization 15-4
Time of Day management on the 7705 SAR-H 15-5
Power management on the 7950 XRS 15-6
15.3 Working with card and card slot objects 15-6
Card provisioning and chassis modes 15-7
15.4 Working with daughter card objects 15-9
IMM daughter cards 15-10
MDA modes for the 7705 SAR 15-10
15.5 Working with bundle objects 15-10
Multilink PPP bundles 15-10
IMA group bundles 15-11
FR group bundles 15-12
15.6 Workflow to manage shelf objects 15-12
15.7 Shelf object configuration procedures 15-14
Procedure 15-1 To configure the device chassis mode 15-14
Procedure 15-2 To configure a VWM shelf for a 7210 SAS 15-15
Procedure 15-3 To configure 7210 SAS dry contact sensors 15-15
Procedure 15-4 To configure switch fabric multicast ingress replication rates 15-16
Procedure 15-5 To configure IMPM overrides 15-17
Procedure 15-6 To enable mixed mode 15-17
Procedure 15-7 To configure timing synchronization 15-18
Procedure 15-8 To configure a 7705 SAR IEEE 1588 PTP clock 15-19
Procedure 15-9 To configure a 7705 SAR IEEE 1588 PTP port 15-20
Procedure 15-10 To configure NTP on supported devices 15-21
Procedure 15-11 To configure a 7705 SAR MW link 15-26
Procedure 15-12 To configure a 7705 SAR MW link member 15-28
Procedure 15-13 To configure 7705 SAR auxiliary alarm definitions 15-30
Procedure 15-14 To configure the IEEE 1588 PTP clock on a 7210 SAS, 7450 ESS, or 7750 SR 15-32
Procedure 15-15 To configure the IEEE 1588 PTP peer of a 7210 SAS, 7450 ESS, or 7750 SR 15-33
Procedure 15-16 To manage an OmniSwitch running configuration 15-34
Procedure 15-17 To configure OmniSwitch health monitoring 15-35
Procedure 15-18 To configure a CCM on a 7950 XRS-20 15-35
Procedure 15-19 To manage the internal fan on a 7210 SAS-D 15-36
Procedure 15-20 To configure a power supply tray 15-37
Procedure 15-21 To configure a power management zone 15-37
Procedure 15-22 To provision a PEQ on a 7950 XRS 15-38

15.8 Card and card slot object configuration procedures 15-38
Procedure 15-23 To assign a card type 15-38
Procedure 15-24 To configure egress WRED queue control on an XCM, IOM 3 or IMM forwarding plane 15-39
Procedure 15-25 To configure IMPM on an XCM, 2 x XP MDA IOM 3, or IMM forwarding plane 15-40
Procedure 15-26 To configure an ingress queue group on a forwarding plane 15-41
Procedure 15-27 To configure NE DDoS protection on a forwarding plane 15-44
Procedure 15-28 To enable named pool mode 15-44
Procedure 15-29 To enable Stable Pool Sizing 15-45
Procedure 15-30 To configure OmniSwitch stacks 15-45
Procedure 15-31 To configure an OmniSwitch CPU temperature threshold 15-46
Procedure 15-32 To configure a CPM on a 7950 XRS 15-46
15.9 Daughter card slot object configuration procedures 15-47
Procedure 15-33 To configure an MDA 15-48
Procedure 15-34 To configure IMPM on an MDA 15-54
Procedure 15-35 To view the operational multicast channel properties of an MDA 15-55
Procedure 15-36 To configure a 7705 SAR module card 15-56
15.10 Bundle configuration procedures 15-59
Procedure 15-37 To create an FR group bundle 15-59
Procedure 15-38 To modify an FR group bundle 15-60
Procedure 15-39 To create an IMA group bundle 15-62
Procedure 15-40 To modify an IMA group bundle 15-64
Procedure 15-41 To create an MLPPP bundle 15-65
Procedure 15-42 To modify an MLPPP bundle 15-67
Procedure 15-43 To configure an MLPPP bundle for multiclass service transmission 15-68
Procedure 15-44 To configure an MLPPP bundle as a network interface on a channelized ASAP MDA 15-70

16 — Port and channel object configuration 16-1

16.1 Port and channel object configuration overview 16-2
16.2 Working with port and channel objects 16-2
Digital diagnostics monitoring 16-5
Tagged and untagged VLAN ports 16-5
Connection termination points for services and interfaces 16-7
STS-3 to STS-192 clear channel 16-7
DS3 clear channel 16-7
DS0 channel groups 16-7
Ethernet ports 16-8
PoE 16-10
PoE on the 7705 SAR-H 16-11
Moving and copying SAPs between ports 16-11
SONET/SDH and TDM port encapsulation 16-13
SONET clear channel applications 16-13
TDM channelization and clear channel applications 16-14
ATM encapsulation 16-16

16.3 SONET and SDH sub-channel applications and structure 16-18
SONET DS3 payload 16-18
SONET VT1.5 and VT2 payloads 16-19
SONET sub-channel syntax 16-20
Comparison of SONET and SDH hierarchies 16-21
SDH AU-4 and AU-3 sub-channel applications 16-22
SDH TU3 payload 16-22
SDH E3 or DS3 payload 16-23
SDH TU11 and TU12 payloads 16-24
16.4 Workflow to manage port objects 16-25
16.5 Workflow to manage channel objects 16-26
16.6 Port configuration procedures 16-27
Procedure 16-1 To configure Ethernet ports 16-27
Procedure 16-2 To change the port mode 16-39
Procedure 16-3 To migrate SAPs from access mode to hybrid mode 16-40
Procedure 16-4 To configure the 5620 SAM to retain non-default port MTU values 16-41
Procedure 16-5 To copy or move L2 SAPs between ports 16-42
Procedure 16-6 To move L3 SAPs within or between ports on the same NE 16-45
Procedure 16-7 To move L3 subscriber interface SAPs between ports on the same NE 16-48
Procedure 16-8 To add a queue group to an Ethernet port 16-51
Procedure 16-9 To configure SONET ports 16-54
Procedure 16-10 To configure an HSMDA override 16-55
Procedure 16-11 To configure TDM DS3 ports 16-56
Procedure 16-12 To configure serial ports 16-57
Procedure 16-13 To configure PW ports 16-57
Procedure 16-14 To configure a 7210 SAS-M channelized TDM DS1 or E1 port 16-58
Procedure 16-15 To assign policies to a 7210 SAS Ethernet port 16-59
Procedure 16-16 To create a 7210 SAS SHG 16-61
Procedure 16-17 To configure a virtual Ethernet port on a 7705 SAR 2-port ring MDA 16-62
Procedure 16-18 To configure PoE ports on a 7210 SAS-T ETR 16-63
Procedure 16-19 To configure PoE ports on a 7705 SAR-H 16-64
Procedure 16-20 To configure PoE ports on a 7705 SAR-W daughter card 16-65
Procedure 16-21 To configure a 7705 SAR ASAP channelized TDM port 16-66
Procedure 16-22 To configure a 7710 SR channelized TDM DS1 or E1 port 16-67
Procedure 16-23 To configure OmniSwitch Ethernet ports 16-68
Procedure 16-24 To configure OmniSwitch PoE Ports 16-72
16.7 Channel and framing link configuration procedures 16-72
Procedure 16-25 To configure SONET clear channels 16-72
Procedure 16-26 To perform a bulk channel creation on ports that support multiple sub-channels 16-74
Procedure 16-27 To configure SONET sub-channels 16-75
Procedure 16-28 To configure SDH sub-channels 16-77
Procedure 16-29 To create VT15 (TU11) or VT2 (TU12) sub-channels 16-79
Procedure 16-30 To create TDM DS1 or E1 channels 16-81

Procedure 16-31 To configure TDM DS1 or E1 channels 16-83
Procedure 16-32 To create serial channels..... 16-85
Procedure 16-33 To create TDM DS3 channels..... 16-87
Procedure 16-34 To configure TDM DS3 channels 16-89
Procedure 16-35 To configure a DS3/E3 channel as a network interface on a channelized ASAP MDA 16-94
Procedure 16-36 To configure an L3 interface on a DS3/E3 channel on a channelized ASAP MDA 16-96
Procedure 16-37 To configure a PVC 16-97
Procedure 16-38 To create an ILMI link..... 16-98
Procedure 16-39 To configure an ILMI link 16-100

17 — Inventory management 17-1

17.1 Inventory management overview..... 17-2
17.2 Sample inventory management workflow 17-5
17.3 Workflow to manage inventory 17-6
17.4 Inventory management procedures 17-7
Procedure 17-1 To list and sort inventory data..... 17-7
Procedure 17-2 To save inventory output in HTML format 17-8
Procedure 17-3 To save inventory output in CSV format..... 17-9
Procedure 17-4 To save a filter 17-9
Procedure 17-5 To inventory CLEI codes for managed device objects..... 17-9
Procedure 17-6 To inventory card software versions for a managed device 17-10
Procedure 17-7 To inventory port types for a managed device..... 17-11
Procedure 17-8 To inventory shelf data for a managed device 17-12
Procedure 17-9 To inventory all managed CCMs..... 17-13
Procedure 17-10 To inventory all managed cards..... 17-13
Procedure 17-11 To inventory all managed fan trays..... 17-14
Procedure 17-12 To inventory all managed flash memory..... 17-14
Procedure 17-13 To inventory all managed physical links 17-15
Procedure 17-14 To inventory all managed ports 17-16
Procedure 17-15 To inventory all managed power supply trays 17-16
Procedure 17-16 To inventory all managed processors..... 17-17
Procedure 17-17 To inventory all managed shelves..... 17-18
Procedure 17-18 To inventory all management ports 17-18
Procedure 17-19 To collect inventory data for network device SLA audits 17-19

18 — Card migration 18-1

18.1 Card migration management overview 18-2
Restrictions 18-2
18.2 Workflow to manage card migration 18-3
18.3 Card migration management procedures..... 18-4
Procedure 18-1 To create a card migration event 18-4
Procedure 18-2 To execute a saved card migration event..... 18-6
Procedure 18-3 To delete a card migration event 18-6

19 — TCA 19-1

19.1 TCA overview 19-2
Statistics counters 19-2
TCA configuration example 19-3
19.2 Workflow to configure TCA 19-4
19.3 TCA management procedures 19-4
Procedure 19-1 To configure a custom TCA profile 19-5
Procedure 19-2 To configure a TCA policy 19-6
Procedure 19-3 To apply a TCA policy to objects using the object properties forms 19-9
Procedure 19-4 To delete a TCA policy 19-10

20 — Bulk operations 20-1

20.1 Bulk operations overview 20-2
20.2 Workflow to manage bulk operations 20-2
20.3 Bulk operations procedures 20-2
Procedure 20-1 To create a bulk change 20-3
Procedure 20-2 To modify a bulk change 20-5
Procedure 20-3 To execute a bulk change 20-5
Procedure 20-4 To view executed batch information 20-6
Procedure 20-5 To stop one or more bulk changes 20-7
Procedure 20-6 To delete a bulk change 20-7

21 — Auto-provision 21-1

21.1 Auto-provision overview 21-2
21.2 Workflow to configure network devices using auto-provision 21-4
21.3 Auto-provision procedures 21-4
Procedure 21-1 To configure a source template 21-4
Procedure 21-2 To configure a target template 21-7
Procedure 21-3 To apply a target template to an unprovisioned NE 21-8

Network management

22 — NE routing and forwarding 22-1

22.1 NE routing and forwarding overview 22-2
L3 network interfaces 22-2
Routing protocols 22-4
LLDP 22-5
Routing policies 22-7
Cflowd 22-11
Shared Risk Link Group policies 22-11
22.2 Network domain overview 22-12
22.3 Workflow to configure NE routing and forwarding 22-12
22.4 Workflow to configure network domains 22-14

22.5 NE routing and forwarding configuration procedures 22-15
Procedure 22-1 To configure a routing instance or a VRF instance 22-15
Procedure 22-2 To configure local DHCPv4 server on a routing instance 22-23
Procedure 22-3 To configure local DHCPv6 server on a routing instance 22-28
Procedure 22-4 To perform a Force Partner Down action on a local DHCP server failover 22-31
Procedure 22-5 To configure a routing instance on an OmniSwitch 22-32
OmniSwitch DHCP relay and snooping 22-33
Procedure 22-6 To configure a UDP relay service, DHCP snooping, and DHCP Option 82 on OmniSwitch routing instances 22-34
Procedure 22-7 To configure a RADIUS server on a routing instance 22-36
Procedure 22-8 To configure a RADIUS proxy server on a routing instance 22-36
Procedure 22-9 To create an L3 interface 22-38
Procedure 22-10 To configure an L3 interface 22-47
Procedure 22-11 To create a L3 interface on an OmniSwitch 22-50
Procedure 22-12 To configure L3 interfaces on an OmniSwitch 22-51
Procedure 22-13 To create a static route 22-51
Procedure 22-14 To configure a static route on an OmniSwitch 22-52
Procedure 22-15 To configure a routing policy statement 22-53
Procedure 22-16 To configure a prefix list policy 22-59
Procedure 22-17 To configure a community policy 22-60
Procedure 22-18 To configure a damping policy 22-62
Procedure 22-19 To configure an AS Path policy 22-63
Procedure 22-20 To configure an AS Path Group policy 22-64
Procedure 22-21 To configure an MPLS administrative group policy 22-65
Procedure 22-22 To configure a Shared Risk Link Group policy 22-67
Procedure 22-23 To create a static configuration for a SRLG Policy 22-68
Procedure 22-24 To view network resources 22-70
Procedure 22-25 To view a routing instance or related object 22-71
Procedure 22-26 To view routing policy usage 22-71
Procedure 22-27 To view DHCPv6 leases 22-72
Procedure 22-28 To view DHCPv6 log events 22-73
Procedure 22-29 To view a routing policy from a CLI session 22-74
Procedure 22-30 To list MVPN Extranet objects for a NE 22-75
Procedure 22-31 To display IOM/IMM Label FIB information 22-76
Procedure 22-32 To display ECMP/LAG hashing of Epipe services 22-76
22.6 Network domain configuration procedures 22-78
Procedure 22-33 To create a network domain 22-78
Procedure 22-34 To associate a network interface with a network domain 22-78
Procedure 22-35 To remove a network interface from a network domain 22-79
Procedure 22-36 To associate a service tunnel with a network domain 22-79
Procedure 22-37 To remove a service tunnel from a network domain 22-79
Procedure 22-38 To delete a network domain 22-80

23 — Protocol configuration 23-1

23.1 Protocol configuration overview 23-3
IPv6 support 23-3
BGP 23-6
MP-BGP 23-8
RIP 23-8
LDP 23-9
IS-IS 23-11
OSPF 23-13
RSVP 23-14
L2TP 23-16
PIM 23-19
IGMP 23-22
MSDP 23-22
MLD 23-23
Bridging 23-23
WPP 23-24
23.2 Workflow to configure protocols 23-24
23.3 Workflow to configure BGP 23-25
23.4 Workflow to configure RIP 23-26
23.5 Workflow to configure LDP 23-26
23.6 Workflow to configure IS-IS 23-26
23.7 Workflow to configure OSPFv2 and OSPFv3 23-27
23.8 Workflow to configure RSVP 23-27
23.9 Workflow to configure L2TP 23-27
23.10 Workflow to configure PIM 23-28
23.11 Workflow to configure IGMP 23-28
23.12 Workflow to configure MSDP 23-29
23.13 Workflow to configure MLD 23-29
23.14 Workflow to configure bridging on an OmniSwitch device 23-29
23.15 Workflow to configure WPP 23-29
23.16 BGP configuration procedures 23-30
Procedure 23-1 To enable BGP on a routing instance 23-31
Procedure 23-2 To configure global-level BGP 23-31
Procedure 23-3 To configure a BGP confederation 23-37
Procedure 23-4 To configure peer-group-level BGP 23-38
Procedure 23-5 To configure peer-level BGP 23-43
Procedure 23-6 To enable or disable BGP peering 23-47
Procedure 23-7 To perform a routing policy test 23-48
23.17 RIP configuration procedures 23-49
Procedure 23-8 To enable RIP on a routing instance 23-49
Procedure 23-9 To configure global-level RIP 23-49
Procedure 23-10 To configure group-level RIP 23-51
Procedure 23-11 To configure interface-level RIP 23-52
23.18 LDP configuration procedures 23-52
Procedure 23-12 To enable LDP on a routing instance 23-53
Procedure 23-13 To configure global-level LDP 23-53
Procedure 23-14 To configure an LDP interface 23-57
Procedure 23-15 To configure an LDP peer 23-58
Procedure 23-16 To configure an LDP targeted peer 23-60
Procedure 23-17 To configure ECMP for LDP routing 23-62
Procedure 23-18 To view the LDP session information 23-63

23.19 IS-IS configuration procedures 23-64
Procedure 23-19 To enable IS-IS on a routing instance..... 23-65
Procedure 23-20 To configure IS-IS on a routing instance 23-66
Procedure 23-21 To configure an IS-IS link group on a routing instance..... 23-70
Procedure 23-22 To configure an IS-IS NET address..... 23-71
Procedure 23-23 To configure an IS-IS interface 23-72
23.20 OSPF configuration procedures 23-75
Procedure 23-24 To enable OSPF on a routing instance..... 23-76
Procedure 23-25 To create an OSPF area..... 23-77
Procedure 23-26 To create an OSPF neighbor on an OmniSwitch..... 23-78
Procedure 23-27 To add a Layer 3 interface to an OSPF router 23-79
Procedure 23-28 To create an OSPF area range 23-81
Procedure 23-29 To create a virtual link 23-81
Procedure 23-30 To configure OSPF on a default routing instance or a VRF routing instance 23-83
Procedure 23-31 To add a router to an OSPF area 23-86
23.21 RSVP configuration procedures 23-87
Procedure 23-32 To configure RSVP on a routing instance 23-87
Procedure 23-33 To configure an RSVP interface 23-89
23.22 L2TP configuration procedures 23-90
Procedure 23-34 To configure L2TP on a routing instance..... 23-91
Procedure 23-35 To view L2TP tunnels and tunnel endpoints..... 23-95
Procedure 23-36 To view L2TP tunnel instance endpoints on a subscriber instance 23-96
Procedure 23-37 To view L2TP sessions..... 23-97
Procedure 23-38 To view PPP sessions 23-97
23.23 PIM configuration procedures 23-98
Procedure 23-39 To enable PIM on a routing instance..... 23-98
Procedure 23-40 To configure PIM on a routing instance 23-99
Procedure 23-41 To create a PIM site on a VPRN routing instance 23-104
Procedure 23-42 To configure Anycast PIM on a router 23-113
Procedure 23-43 To create a PIM interface on a base routing instance or VPRN routing instance..... 23-116
Procedure 23-44 To view an mVPN P2MP LSP object 23-118
23.24 IGMP configuration procedures 23-119
Procedure 23-45 To enable IGMP on a router..... 23-119
Procedure 23-46 To configure an IGMP site on a router..... 23-119
Procedure 23-47 To configure IGMP on an OmniSwitch 23-122
Procedure 23-48 To create an IGMP interface..... 23-122
Procedure 23-49 To turn up or shut down an IGMP interface 23-124
Procedure 23-50 To view IGMP multicast reporting statistics for an IGMP site..... 23-125
Procedure 23-51 To view IGMP source statistics 23-125
23.25 MSDP configuration procedures..... 23-126
Procedure 23-52 To enable MSDP on a router 23-127
Procedure 23-53 To configure global-level MSDP..... 23-127
Procedure 23-54 To configure group-level MSDP 23-128
Procedure 23-55 To configure an MSDP source 23-131
Procedure 23-56 To configure peer-level MSDP 23-131
Procedure 23-57 To configure group-peer-level MSDP 23-133
Procedure 23-58 To enable or disable MSDP peering 23-134

23.26 MLD configuration procedures 23-134
Procedure 23-59 To enable MLD on a routing instance 23-135
Procedure 23-60 To configure MLD on a routing instance or VPRN routing instance 23-135
Procedure 23-61 To create an MLD interface on a base routing instance or VPRN routing instance 23-137
Procedure 23-62 To configure an MLD interface on an IES L3 access interface 23-138
23.27 Bridging configuration procedures 23-140
Procedure 23-63 To configure bridging on an OmniSwitch 23-140
Procedure 23-64 To release a violated OmniSwitch LPS port 23-147
23.28 WPP configuration procedure 23-148
Procedure 23-65 To create a web portal 23-148

24 — NAT 24-1

24.1 NAT overview 24-2
L2-aware NAT 24-3
Large-scale NAT 24-3
Static port forwarding 24-4
NAT pools 24-4
NAT policies 24-5
ISA-NAT groups 24-5
NAT Destinations 24-5
NAT 64 24-5
DS Lite 24-5
Deterministic NAT 24-6
24.2 Workflow to configure NAT 24-6
24.3 NAT configuration procedures 24-6
Procedure 24-1 To configure an ISA-NAT group 24-7
Procedure 24-2 To configure a NAT policy 24-8
Procedure 24-3 To configure NAT on a routing instance 24-9
Procedure 24-4 To configure a NAT deterministic script on a remote server 24-15
Procedure 24-5 To create an IPFIX export policy 24-16
Procedure 24-6 To view reserved IP address and reserved block information on an ISA-NAT group 24-17
Procedure 24-7 To view ISA-NAT object information 24-18
Procedure 24-8 To configure statistics on an ISA-NAT group 24-18
Procedure 24-9 To plot LSN subscriber host statistics 24-20
Procedure 24-10 To start or stop a NAT address-pool drain operation 24-21

25 — MPLS 25-1

25.1 MPLS overview 25-2
LSPs 25-2
25.2 Sample MPLS configuration 25-11
25.3 Workflow to configure MPLS 25-12
25.4 MPLS procedures 25-13
Procedure 25-1 To enable MPLS on a routing instance 25-13
Procedure 25-2 To configure an MPLS instance 25-14

Procedure 25-3 To create an MPLS interface 25-16
Procedure 25-4 To create an MPLS path 25-18
Procedure 25-5 To view an MPLS path 25-20
Procedure 25-6 To create a static LSP 25-21
Procedure 25-7 To view and configure a static LSP 25-22
Procedure 25-8 To create a dynamic LSP 25-23
Procedure 25-9 To configure a dynamic LSP 25-28
Procedure 25-10 To create a dynamic LSP from a tunnel template 25-30
Procedure 25-11 To list dynamic LSPs 25-32
Procedure 25-12 To run an OAM validation test for a dynamic LSP 25-32
Procedure 25-13 To create a Point-to-Multipoint LSP 25-32
Procedure 25-14 To create a Manual Bypass LSP 25-36
Procedure 25-15 To configure a Manual Bypass LSP 25-39
Procedure 25-16 To configure an LSP path 25-40
Procedure 25-17 To create an LSP path using a tunnel template 25-43
Procedure 25-18 To configure an LSP Path optimization policy 25-44
Procedure 25-19 To terminate an LSP Path optimization policy that is in progress 25-46
Procedure 25-20 To view LSP Path optimization policy results 25-47
Procedure 25-21 To view detour and bypass path information 25-48
Procedure 25-22 To view exclude route object information 25-49
Procedure 25-23 To create an LSP template for MVPN 25-50
Procedure 25-24 To view LSP templates for MVPN created using CLI 25-52
Procedure 25-25 To view LSPs created by one-hop P2P and mesh P2P templates 25-53
Procedure 25-26 To list and view MPLS objects 25-53

26 — MPLS-TP 26-1

26.1 MPLS-TP overview 26-2
Proactive OAM 26-2
26.2 Simplified provisioning 26-3
26.3 Workflow to configure MPLS-TP 26-3
26.4 MPLS-TP procedures 26-4
Procedure 26-1 To enable MPLS-TP on a routing instance 26-4
Procedure 26-2 To configure an MPLS-TP instance 26-5
Procedure 26-3 To create an MPLS-TP BFD template policy 26-5
Procedure 26-4 To configure a proactive OAM template on an MPLS-TP instance 26-6
Procedure 26-5 To configure a protection template on an MPLS-TP instance 26-7
Procedure 26-6 To create an MPLS-TP LSP 26-7
Procedure 26-7 To create an MPLS-TP LSR cross-connect path 26-10
Procedure 26-8 To create a bidirectional MPLS-TP LSP 26-12

27 — Service tunnels 27-1

27.1 Service tunnel overview 27-2
Tunnel selection profiles 27-3
27.2 IP/MPLS service tunnels 27-3
IP/MPLS service tunnels design considerations 27-4
Class-based forwarding 27-5

27.3 Ethernet (G.8031) tunnels 27-5
Transit services 27-6
27.4 Ethernet (G.8032) rings 27-7
ERP topology 27-7
Supported ERP service types 27-8
Automatic Ethernet ring creation 27-8
Auditing Ethernet rings 27-9
Service provisioning on Ethernet (G.8032) rings 27-9
27.5 Workflow to configure service tunnels 27-10
27.6 Workflow to configure Ethernet (G.8032) rings 27-11
27.7 Configuring service tunnel procedures 27-11
Procedure 27-1 To create an IP/MPLS service tunnel 27-11
Procedure 27-2 To create an SDP using a tunnel template 27-18
Procedure 27-3 To create a tunnel selection profile 27-19
Procedure 27-4 To create or configure an Ethernet tunnel endpoint 27-21
Procedure 27-5 To create an Ethernet tunnel 27-24
Procedure 27-6 To create or configure an Ethernet Ring Element 27-27
Procedure 27-7 To create or configure an Ethernet Ring Element on an OmniSwitch NE 27-30
Procedure 27-8 To create an Ethernet (G.8032) ring 27-34
Procedure 27-9 To create an Ethernet (G.8032v2) ring on OmniSwitch NEs 27-42
Procedure 27-10 To configure a transit service on an Ethernet ring 27-44
Procedure 27-11 To discover service tunnels 27-46
Procedure 27-12 To discover flow-through services 27-47
Procedure 27-13 To view and manage service tunnels and tunnel elements 27-48
Procedure 27-14 To view the service tunnel topology 27-49
Procedure 27-15 To run an OAM validation test on a service tunnel 27-50
Procedure 27-16 To perform an Ethernet (G.8032) ring audit 27-51

28 — Lawful Intercept 28-1

28.1 Lawful Intercept overview 28-2
Security 28-3
28.2 Workflow to configure LI 28-4
28.3 5620 SAM LI configuration procedures 28-5
Procedure 28-1 To create an LI user account on the 5620 SAM 28-6
Procedure 28-2 To create an additional NE LI user account using the 5620 SAM GUI 28-8
Procedure 28-3 To create an NE LI user profile using CLI 28-10
Procedure 28-4 To create an LI user account on an NE using a CLI 28-11
Procedure 28-5 To configure NE LI user security 28-13
Procedure 28-6 To synchronize the global 5620 SAM NE user configuration profile with the local NE user configuration profile 28-15
Procedure 28-7 To configure an LI mediation policy 28-15
Procedure 28-8 To enable NE discovery for LI 28-16
Procedure 28-9 To configure the LI Filter Lock 28-18
Procedure 28-10 To configure LI on a specific NAT subscriber 28-18
Procedure 28-11 To enable or disable the use of a secure channel for LI users 28-20

29 — IPsec 29-1

29.1 IPsec overview 29-2
IPv6 IPsec 29-3
BFD 29-3
29.2 IPsec VPN 29-4
Tunnel types 29-4
Typical applications for IPsec corporate services 29-4
29.3 Multi-chassis IPsec 29-7
29.4 Sample video wholesale IPsec configuration 29-7
29.5 Workflow to configure and manage an IPsec configuration 29-8
29.6 Workflow to configure and manage an IPsec configuration using the IPsec VPN 29-9
29.7 Workflow to enable BFD over a static LAN-to-LAN IPsec tunnel 29-9
29.8 General IPsec procedures 29-10
Procedure 29-1 To configure an IKE policy 29-10
Procedure 29-2 To configure an IPsec transform 29-11
Procedure 29-3 To create an IPsec static security association 29-12
Procedure 29-4 To create an IPsec tunnel template 29-13
Procedure 29-5 To create an IPsec security policy 29-13
Procedure 29-6 To create a tunnel interface on an IES or VPRN 29-15
Procedure 29-7 To create an IPsec tunnel on a VPRN tunnel interface 29-20
Procedure 29-8 To create an IPsec gateway on an IES or VPRN 29-24
Procedure 29-9 To enable BFD for a static LAN-to-LAN IPsec tunnel 29-26
29.9 IPsec VPN procedures 29-27
Procedure 29-10 To create an IPsec VPN 29-27
Procedure 29-11 To select a service NE site for an IPsec VPN 29-28
Procedure 29-12 To create or select a secure VPRN service for an IPsec VPN 29-29
Procedure 29-13 To create or select a delivery service for an IPsec VPN 29-30
Procedure 29-14 To select a tunnel group for an IPsec VPN 29-32
Procedure 29-15 To assign policies and configurations for a dynamic site-to-site IPsec VPN 29-33
Procedure 29-16 To assign policies and configurations for a dynamic soft client IPsec VPN 29-35
Procedure 29-17 To assign policies and configurations for a static IPsec VPN 29-37

30 — ISA-Video 30-1

30.1 ISA-Video overview 30-2
30.2 Workflow to configure and manage an ISA-Video configuration 30-3
30.3 ISA-Video procedures 30-4
Procedure 30-1 To add a Video interface to a VPRN site 30-4
Procedure 30-2 To add a Video interface to an IES site 30-6
Procedure 30-3 To add a Video interface to a VPLS site 30-8

31 — Alarm management 31-1

31.1 Alarm management overview 31-2
Alarm status, severity, and aggregation 31-6
Alarm thresholds 31-10
Alarm suppression 31-12
Alarm filters 31-13
Filtering alarms for OSS clients using the 5620 SAM GUI 31-13
Correlated alarms 31-13
Automatic purging of alarms 31-15
31.2 Workflow to manage alarms 31-15
31.3 Alarm management procedures 31-17
Procedure 31-1 To configure alarm severity and deletion behavior 31-17
Procedure 31-2 To configure alarm history database management behavior 31-20
Procedure 31-3 To customize the default behavior of specific alarm policies 31-20
Procedure 31-4 To display the Additional Text Find button on object properties forms 31-21
Procedure 31-5 To configure additional text policies 31-22
Procedure 31-6 To set a policy to clear an alarm that is not implicitly cleared 31-25
Procedure 31-7 To configure alarm filters for OSS clients using the 5620 SAM GUI 31-25
Procedure 31-8 To reload all alarms from the historical alarm database 31-27
Procedure 31-9 To enable or disable audible alarms 31-28
Procedure 31-10 To enable or disable the display of alarm flags in the alarm window 31-28
Procedure 31-11 To enable or disable the display of correlated alarms in the alarm window 31-29
Procedure 31-12 To enable or disable the display of alarmed equipment in navigation trees for the View Alarmed Object function 31-30
Procedure 31-13 To view and manage network alarms in the Alarm window 31-30
Procedure 31-14 To view and manage object alarms on object properties forms 31-33
Procedure 31-15 To view and manage alarms using the Alarm Info form 31-36
Procedure 31-16 To create search filters to view specific network alarms 31-38
Procedure 31-17 To acknowledge alarms using the contextual menu on alarm lists 31-39
Procedure 31-18 To acknowledge alarms using the Alarm Info form 31-40
Procedure 31-19 To manually promote or demote the severity of an alarm 31-42
Procedure 31-20 To list alarms received during a specified time period 31-43
Procedure 31-21 To search for alarms received during a specified time period 31-44
Procedure 31-22 To pause the dynamic alarm list from scrolling when viewing alarms 31-44

Procedure 31-23 To copy alarm information to the clipboard 31-45
Procedure 31-24 To view network alarm statistics 31-46
Procedure 31-25 To review historical alarm records 31-46
Procedure 31-26 To view the source object of an historical alarm 31-47
Procedure 31-27 To save lists of logged historical alarm records 31-48

32 — OAM diagnostic tests 32-1

32.1 OAM diagnostic tests overview 32-2
Ethernet CFM 32-4
MTU ping OAM 32-6
Tunnel ping OAM 32-7
Service site ping OAM 32-8
VCCV Ping OAM 32-8
VCCV trace OAM 32-10
LSP Ping OAM 32-10
LSP Trace OAM 32-11
P2MP LSP Ping OAM 32-11
P2MP LSP Trace OAM 32-12
LDP Tree Trace OAM 32-12
MAC ping OAM 32-13
MAC trace OAM 32-14
MAC populate OAM 32-15
MAC purge OAM 32-15
CPE ping 32-16
ANCP loopback 32-16
F5 OAM loopback 32-16
VPRN ping and VPRN trace 32-16
ATM OAM ping 32-16
Multicast FIB ping 32-16
Multicast router information 32-17
Multicast trace 32-17
ICMP ping 32-17
ICMP trace 32-17
OmniSwitch ping and traceroute 32-17
DNS ping 32-18
Service assurance test management and configuration 32-18
32.2 Sample OAM diagnostic test configuration 32-22
32.3 Workflow to use OAM diagnostic tests 32-24
32.4 OSS OAM Test Results file retrieval 32-26
32.5 OAM diagnostic tests procedures 32-26
Procedure 32-1 To create and run an MTU ping OAM diagnostic from a service tunnel 32-27
Procedure 32-2 To create an MTU ping OAM diagnostic from the test manager 32-28
Procedure 32-3 To create and run a tunnel ping OAM diagnostic from a service tunnel 32-29
Procedure 32-4 To create a tunnel ping OAM diagnostic from the test manager 32-31
Procedure 32-5 To create and execute a CFM Global MEG OAM diagnostic 32-31

Procedure 32-6 To create and execute a CFM Continuity Check OAM diagnostic 32-32
Procedure 32-7 To create and execute a CFM loopback diagnostic 32-33
Procedure 32-8 To create and execute a CFM link trace diagnostic 32-37
Procedure 32-9 To create and execute a CFM Eth test diagnostic 32-39
Procedure 32-10 To create and execute a CFM one-way delay diagnostic..... 32-40
Procedure 32-11 To create and execute a CFM two-way delay diagnostic..... 32-42
Procedure 32-12 To create and execute a CFM single-ended loss diagnostic..... 32-45
Procedure 32-13 To create and execute a CFM two-way SLM (Synthetic Loss Measurement) diagnostic 32-47
Procedure 32-14 To configure and run VPRN OAM diagnostics from a service 32-49
Procedure 32-15 To configure and run MAC populate OAM diagnostics 32-54
Procedure 32-16 To configure and run MAC purge OAM diagnostics..... 32-55
Procedure 32-17 To configure and run MAC ping OAM diagnostics 32-56
Procedure 32-18 To configure and run MAC trace OAM diagnostics 32-57
Procedure 32-19 To configure and run CPE ping OAM diagnostics..... 32-59
Procedure 32-20 To configure and run ANCP loopback diagnostics 32-60
Procedure 32-21 To configure and run service site ping OAM diagnostics 32-62
Procedure 32-22 To run the F5 OAM loopback diagnostic..... 32-63
Procedure 32-23 To configure and run VCCV Ping OAM diagnostics 32-63
Procedure 32-24 To configure and run VCCV Trace OAM diagnostics 32-65
Procedure 32-25 To configure and run LSP or MPLS-TP LSP Ping OAM diagnostics 32-66
Procedure 32-26 To configure and run LSP or MPLS-TP LSP Trace OAM diagnostics 32-68
Procedure 32-27 To configure and run P2MP LSP Ping OAM diagnostics 32-70
Procedure 32-28 To configure and run P2MP LSP Trace OAM diagnostics 32-74
Procedure 32-29 To configure and run LDP Tree Trace OAM diagnostics 32-75
Procedure 32-30 To configure and run multicast router information OAM diagnostics 32-76
Procedure 32-31 To configure and run multicast trace OAM diagnostics 32-77
Procedure 32-32 To configure and run multicast FIB ping OAM diagnostics 32-78
Procedure 32-33 To configure and run an ATM OAM ping..... 32-79
Procedure 32-34 To configure an ATM OAM loopback 32-80
Procedure 32-35 To configure and run an ICMP ping 32-81
Procedure 32-36 To configure and run an ICMP trace 32-82
Procedure 32-37 To configure and run a DNS ping..... 32-83
Procedure 32-38 To create an OmniSwitch OAM CLI script 32-85
Procedure 32-39 To configure an advanced loopback test on an OmniSwitch port..... 32-89
Procedure 32-40 To configure and run an OmniSwitch OAM ping..... 32-90

Procedure 32-41 To configure and run an OmniSwitch OAM traceroute 32-92
Procedure 32-42 To configure an 802.3ah EFM OAM diagnostic 32-93
Procedure 32-43 To configure an 802.3ah EFM OAM diagnostic on an OmniSwitch at the NE or port level 32-98
Procedure 32-44 To view OAM diagnostic test results 32-103
Procedure 32-45 To interpret OAM diagnostic results 32-112
Procedure 32-46 To configure threshold-crossing alarms on NE-schedulable OAM tests 32-120
Procedure 32-47 To configure NM threshold-crossing alarms on non-NE-schedulable OAM tests 32-121
Procedure 32-48 To edit an OAM diagnostic test 32-122
Procedure 32-49 To delete an OAM diagnostic test 32-123
Procedure 32-50 To set STM managed device test limits 32-123

33 — VRRP 33-1

33.1 VRRP overview 33-2
VR 33-3
Master router 33-4
Owner and non-owner VRRP instances 33-4
VRRP types 33-5
Primary addresses 33-5
Backup addresses 33-5
VRRP message authentication 33-5
33.2 Workflow to configure VRRP 33-5
33.3 VRRP management procedures 33-6
Procedure 33-1 To create a VR 33-6
Procedure 33-2 To create and configure a VRRP instance 33-6
Procedure 33-3 To add a VRRP instance 33-9
Procedure 33-4 To modify a VR or VRRP instance 33-9
Procedure 33-5 To view the status of a VR 33-10
Procedure 33-6 To delete a VRRP instance 33-11
Procedure 33-7 To delete a VR 33-11

34 — APS 34-1

34.1 APS overview 34-2
Bidirectional mode 34-3
Unidirectional mode 34-3
Switching modes 34-4
MLPPP 34-4
APS port configurations 34-5
SC APS 34-6
MC APS 34-6
APS on channelized ASAP MDAs 34-7
APS on channelized CES MDAs 34-7
APS on multilink bundles 34-7
1+1 APS configuration example 34-8
Configuring SAPs on APS-protected ports 34-9
34.2 Workflow to manage APS 34-9

34.3 APS management procedures 34-10
Procedure 34-1 To create an SC APS group 34-10
Procedure 34-2 To create an MC APS group 34-12
Procedure 34-3 To create an SC APS IMA or MLPPP bundle 34-15
Procedure 34-4 To create an MC APS MLPPP bundle 34-20
Procedure 34-5 To change the operational state of an SC APS channel 34-24
Procedure 34-6 To delete an SC APS group 34-24
Procedure 34-7 To delete an SC APS bundle 34-25
Procedure 34-8 To delete an MC APS group or bundle 34-25

35 — lightRadio Wi-Fi 35-1

35.1 lightRadio Wi-Fi 35-2
Migrant user handling 35-3
35.2 Workflow to configure lightRadio Wi-Fi 35-4

36 — MC peer groups 36-1

36.1 MC peer groups overview 36-2
36.2 Workflow to manage MC peer groups 36-3
36.3 MC peer groups management procedures 36-3
Procedure 36-1 To configure an MC peer group 36-3
Procedure 36-2 To configure an MC peer 36-6
Procedure 36-3 To perform an on-demand protocol synchronization between MC peer group members 36-7
Procedure 36-4 To view an MC peer on one NE 36-8
Procedure 36-5 To delete an MC peer group 36-9

37 — MC IPsec 37-1

37.1 MC IPsec overview 37-2
37.2 Workflow to configure and manage MC IPsec 37-2
37.3 MC IPsec management procedures 37-3
Procedure 37-1 To configure MC IPsec on an MC peer group 37-4
Procedure 37-2 To create an MC IPsec group 37-6
Procedure 37-3 To configure MC IPsec on a VPRN tunnel interface 37-8
Procedure 37-4 To configure MC IPsec on an IES or VPRN L3 access interface 37-9
Procedure 37-5 To perform an MC IPsec switchover 37-10
Procedure 37-6 To view an MC IPsec peer on an NE 37-11
Procedure 37-7 To configure an MC IPsec peer site 37-11

38 — MC endpoint groups 38-1

38.1 MC endpoint groups overview 38-2
BFD 38-2
38.2 Workflow to manage MC endpoint groups 38-2
38.3 MC endpoint groups management procedures 38-3
Procedure 38-1 To configure an MC endpoint group 38-3
Procedure 38-2 To modify an MC endpoint group 38-4
Procedure 38-3 To view an MC endpoint peer on one NE 38-5

Procedure 38-4 To delete an MC endpoint group 38-6

39 — MC LAG groups 39-1

39.1 MC LAG groups overview 39-2
MC synchronization 39-2
39.2 Workflow to manage MC LAG groups 39-2
39.3 MC LAG groups management procedures 39-3
Procedure 39-1 To create an MC LAG group 39-3
Procedure 39-2 To configure an MC LAG group member 39-5
Procedure 39-3 To configure an MC LAG peer on one NE 39-6
Procedure 39-4 To delete an MC LAG group 39-7
39.4 MC AOS groups overview 39-7
39.5 Workflow to manage MC AOS groups 39-8
39.6 MC AOS groups management procedures 39-8
Procedure 39-5 To create an MC AOS group 39-8
Procedure 39-6 To create an MC AOS VFLink Group 39-10
Procedure 39-7 To create an MC AOS LAG Group 39-11
Procedure 39-8 To configure an MC AOS group member 39-12

40 — MC synchronization groups 40-1

40.1 MC synchronization groups overview 40-2
MC synchronization and dual-homed L2/L3 CO 40-2
40.2 Workflow to manage MC synchronization groups 40-3
40.3 MC synchronization groups management procedures 40-3
Procedure 40-1 To create an MC synchronization group 40-3
Procedure 40-2 To configure protocol synchronization between MC peer group members 40-5
Procedure 40-3 To view an MC synchronization peer on one NE 40-5
Procedure 40-4 To delete an MC synchronization group 40-6

41 — MC ring groups 41-1

41.1 MC ring groups overview 41-2
Steady-state condition 41-3
Broken ring condition 41-4
Object relationships 41-5
MC ring group and redundant VLL Epipe access operation 41-6
MC ring groups and subscriber hosts 41-7
41.2 Workflow to manage MC ring groups 41-7
41.3 MC ring groups management procedures 41-10
Procedure 41-1 To create an MC ring group 41-10
Procedure 41-2 To configure L3 forwarding from a VPLS or MVPLS to an IES or VPRN service 41-12
Procedure 41-3 To configure an MC ring group for redundant VLL Epipe access 41-13
Procedure 41-4 To turn up the MC rings in an MC ring group 41-14
Procedure 41-5 To view the operational status of MC ring group components 41-15
Procedure 41-6 To configure an MC ring peer on one NE 41-17
Procedure 41-7 To delete an MC ring group 41-19

Policy management

42 — Policies overview 42-1

42.1 Policies overview 42-2
Policy types 42-2
Global policies 42-12
Policy distribution 42-13
Policy audits 42-14
Policy overrides 42-15
42.2 Workflow to create and assign policies 42-16
42.3 Policies procedures 42-17
Procedure 42-1 To distribute a policy 42-17
Procedure 42-2 To distribute multiple policies 42-21
Procedure 42-3 To create a policy distribution group 42-23
Procedure 42-4 To modify a policy 42-24
Procedure 42-5 To delete a policy 42-25
Procedure 42-6 To copy or overwrite a policy 42-26
Procedure 42-7 To synchronize a policy 42-27
Procedure 42-8 To perform a policy audit for policy groups and types 42-28
Procedure 42-9 To perform a policy audit for multiple global policies with same type 42-30
Procedure 42-10 To perform a policy audit for global policy 42-31
Procedure 42-11 To configure a policy audit schedule 42-33
Procedure 42-12 To identify differences between a global and local policy or two local policies 42-35
Procedure 42-13 To configure the maximum policy objects per deployer 42-37
Procedure 42-14 To configure the maximum number of tasks for distribution 42-38

43 — QoS policies 43-1

43.1 QoS policies overview 43-2
Access ingress policies 43-2
Access egress policies 43-5
Network policies 43-6
Network queue policies 43-7
Slope policies 43-7
HSMDA slope policies 43-8
Shared-queue policies 43-8
Scheduler policies 43-10
HSMDA scheduler policies 43-12
Port scheduler policies 43-12
Policer control policies 43-13
Named buffer pool policies 43-14
Queue Group Template policies 43-14
7705 SAR fabric profiles 43-15
HSMDA pool policies 43-16
ATM QoS policies 43-16

MC MLPPP ingress and egress QoS profiles 43-16
MCFR ingress and egress QoS profiles 43-16
OmniSwitch QoS policies 43-16
7210 SAS QoS policies 43-17
43.2 Workflow to configure policer control hierarchy 43-18
43.3 Workflow to configure 5620 SAM named buffer pools 43-19
43.4 QoS policies procedures 43-20
Procedure 43-1 To configure an access ingress policy 43-20
Procedure 43-2 To configure a 7210 SAS or 1830 PSS access ingress policy 43-28
Procedure 43-3 To configure a SAP access egress policy 43-33
Procedure 43-4 To configure a 7210 SAS or 1830 PSS port access egress policy 43-41
Procedure 43-5 To configure a 7210 SAS SAP access egress policy 43-43
Procedure 43-6 To configure a network policy 43-45
Procedure 43-7 To configure a 7210 SAS or 1830 PSS network policy 43-47
Procedure 43-8 To configure a WRED slope policy 43-50
Procedure 43-9 To configure a 7210 SAS slope policy 43-52
Procedure 43-10 To configure an HSMDA WRED slope policy 43-54
Procedure 43-11 To configure a 7210 SAS queue management policy 43-56
Procedure 43-12 To configure a network queue policy 43-58
Procedure 43-13 To configure a 7210 SAS or 1830 PSS network queue policy 43-62
Procedure 43-14 To modify a shared-queue policy 43-63
Procedure 43-15 To configure a scheduler policy 43-65
Procedure 43-16 To configure an HSMDA scheduler policy 43-68
Procedure 43-17 To configure an HSMDA WRR policy 43-69
Procedure 43-18 To configure a port scheduler policy 43-71
Procedure 43-19 To configure a 7210 SAS or 1830 PSS port scheduler policy 43-73
Procedure 43-20 To configure a policer control policy 43-74
Procedure 43-21 To configure a port policy 43-75
Procedure 43-22 To configure a named buffer pool policy 43-76
Procedure 43-23 To configure an ingress queue group template policy 43-77
Procedure 43-24 To configure an egress queue group template policy 43-81
Procedure 43-25 To configure an Advanced Configuration policy 43-86
Procedure 43-26 To configure a 7705 SAR fabric profile 43-88
Procedure 43-27 To configure a 7210 SAS remarking policy 43-90
Procedure 43-28 To configure a 7210 MPLS LSP-Exp Map policy 43-91
Procedure 43-29 To configure an HSMDA pool policy 43-92
Procedure 43-30 To configure Q1 pools 43-93
Procedure 43-31 To create an Aggregation Scheduler 43-94
Procedure 43-32 To configure an ANCP MSS static map 43-96
Procedure 43-33 To configure an ATM QoS policy 43-97
Procedure 43-34 To configure an OmniSwitch QoS policy condition 43-98
Procedure 43-35 To configure an OmniSwitch QoS policy action 43-100
Procedure 43-36 To create an OmniSwitch QoS policy 43-101
Procedure 43-37 To create an OmniSwitch QoS list 43-102
Procedure 43-38 To create or configure a MC MLPPP ingress QoS profile 43-104

Procedure 43-39 To create or configure a MC MLPPP egress QoS profile 43-105
Procedure 43-40 To create or configure an MCFR ingress QoS profile .. 43-106
Procedure 43-41 To create or configure an MCFR egress QoS profile ... 43-107
Procedure 43-42 To configure QoS policy overrides on an L2 or L3 access interface 43-108
Procedure 43-43 To configure QoS policy overrides on access ingress policy meters for the 7210 SAS 43-113
Procedure 43-44 To configure QoS policy overrides on access ingress queues for a 7210 SAS-X 43-114

44 — Filter policies 44-1

44.1 Filter policies overview 44-2
Shared filter entries 44-2
SAP and service tunnel forwarding 44-3
Embedded filter policies 44-3
Web portal redirect 44-4
44.2 Filter policies procedures 44-4
Procedure 44-1 To configure an ACL MAC filter policy 44-4
Procedure 44-2 To configure an ACL IP filter policy 44-8
Procedure 44-3 To configure an ACL IPv6 filter policy 44-13
Procedure 44-4 To configure an ACL VLAN filter policy 44-18
Procedure 44-5 To configure an IP Prefix List 44-19
Procedure 44-6 To configure a filter Port List 44-20
Procedure 44-7 To configure a DHCP filter policy 44-21
Procedure 44-8 To configure an LI MAC filter policy 44-24
Procedure 44-9 To configure a Block Reservation policy 44-25
Procedure 44-10 To configure a Filter Log 44-26
Procedure 44-11 To configure a Sys Log 44-28
Procedure 44-12 To copy filter policy filter entries 44-29
Procedure 44-13 To configure embedded and embedding filter policies 44-30

45 — Multicast policies 45-1

45.1 Multicast policies overview 45-2
Egress multicast groups 45-2
Multicast package policies 45-2
Ingress Multicast Bandwidth policy 45-4
Ingress Multicast Info policy 45-4
Ingress Multicast Reporting Destination policy 45-6
7210 Multipoint Bandwidth Management policy 45-6
SSM Translate policy 45-6
45.2 Multicast policies procedures 45-6
Procedure 45-1 To create an egress multicast group policy 45-6
Procedure 45-2 To configure a multicast CAC policy 45-8
Procedure 45-3 To configure an Ingress Multicast Bandwidth policy 45-9
Procedure 45-4 To configure an Ingress Multicast Information policy ... 45-11
Procedure 45-5 To create or edit an ingress multicast reporting destination policy 45-21
Procedure 45-6 To configure a Multicast SSM Translate policy 45-22

Procedure 45-7 To view NE multicast reporting destination statistics 45-23
Procedure 45-8 To view multicast CAC channel statistics 45-24
Procedure 45-9 To configure a multicast package policy 45-25
Procedure 45-10 To configure a 7210 SAS multipoint bandwidth management policy 45-27

46 — Time of day policies 46-1
46.1 Time of day policies overview 46-2
Time range assignment analysis tool 46-2
46.2 Time of day policies procedures 46-2
Procedure 46-1 To configure a time range policy 46-3
Procedure 46-2 To configure a time of day suite 46-4
Procedure 46-3 To perform a time range entry assignment analysis 46-7

47 — VRRP policies 47-1
47.1 VRRP policies overview 47-2
47.2 VRRP policies procedures 47-3
Procedure 47-1 To configure a VRRP priority-control policy 47-3

48 — Auto tunnels policies 48-1
48.1 Auto tunnels policies overview 48-2
Tunnel templates 48-2
Class of Service 48-3
Tunnel groups 48-3
Tunnel policy rules 48-4
48.2 Workflow to configure auto tunnel creation 48-5
48.3 Auto tunnels policies procedures 48-6
Procedure 48-1 To create a rule-based group 48-6
Procedure 48-2 To convert old auto tunnel rules to template-based auto tunnel rules 48-7
Procedure 48-3 To create a mesh or ring topology rule 48-9
Procedure 48-4 To create a hub-and-spoke topology rule 48-11
Procedure 48-5 To import tunnels not managed by topology rules 48-13
Procedure 48-6 To display and delete tunnel elements 48-14
Procedure 48-7 To execute or reapply a topology rule 48-15
Procedure 48-8 To display missing tunnel elements 48-16

49 — AAA policies 49-1
49.1 AAA policies overview 49-2
RADIUS-based accounting policies 49-2
NAT RADIUS accounting policies 49-2
RADIUS server policies 49-2
Accounting on/off groups 49-3
Route download policies 49-3
Subscriber authentication policies 49-3
49.2 Workflow to configure AAA policies 49-3

49.3 AAA policies procedures 49-3
Procedure 49-1 To configure a RADIUS-based accounting policy 49-4
Procedure 49-2 To configure a NAT RADIUS accounting policy 49-7
Procedure 49-3 To configure an L2TP RADIUS accounting policy 49-9
Procedure 49-4 To configure a RADIUS server policy 49-11
Procedure 49-5 To initiate an accounting on/off message from a RADIUS server policy 49-14
Procedure 49-6 To configure an accounting on/off group 49-15
Procedure 49-7 To configure a route download policy 49-16
Procedure 49-8 To configure an ISA RADIUS policy 49-17
Procedure 49-9 To force a route download on an NE 49-17

50 — 802.1x policies 50-1

50.1 802.1x policies overview 50-2
50.2 802.1x policies procedures 50-2
Procedure 50-1 To configure an 802.1X policy 50-2

51 — PBB MRP policies 51-1

51.1 PBB MRP policies overview 51-2
51.2 Workflow to manage PBB MRP policies 51-2
51.3 PBB MRP policies procedures 51-2
Procedure 51-1 To configure a PBB MRP policy 51-2

52 — AOS Ethernet Service policies 52-1

52.1 AOS Ethernet Service policies overview 52-2
52.2 AOS Ethernet Service policies procedures 52-2
Procedure 52-1 To configure an OmniSwitch Ethernet service UNI profile 52-2
Procedure 52-2 To configure an OmniSwitch Ethernet SAP profile 52-3
Procedure 52-3 To configure an OmniSwitch Ethernet service custom L2 profile 52-4
Procedure 52-4 To clear custom L2 profile stats 52-5

53 — Connection profile policies 53-1

53.1 Connection profile policies overview 53-2
7210 SAS VLAN ranges on Epipe SAPs 53-2
53.2 Workflow to manage connection profiles 53-3
53.3 Connection profile policies procedures 53-3
Procedure 53-1 To configure a connection profile policy 53-3
Procedure 53-2 To configure a VLAN range for 7210 SAS Epipe VLL service 53-4

54 — Residential subscriber policies 54-1

54.1 Residential subscriber policies overview 54-2
Subscriber identification policies 54-2
Subscriber profiles 54-3
SLA profiles 54-4

Subscriber explicit maps 54-4
ANCP policies 54-5
Host lockout policies 54-5
Host tracking policies 54-6
Operational states of primary and secondary RADIUS scripts 54-6
Diameter policies 54-6
PPPoE policies 54-7
54.2 Residential subscriber policy management procedures 54-8
Procedure 54-1 To configure a subscriber identification policy 54-9
Procedure 54-2 To configure an ANCP policy 54-12
Procedure 54-3 To configure a PPPoE policy 54-13
Procedure 54-4 To configure a PPP policy 54-15
Procedure 54-5 To configure an MSAP policy 54-17
Procedure 54-6 To configure a host tracking policy 54-20
Procedure 54-7 To configure a category map policy 54-21
Procedure 54-8 To configure a credit control policy 54-24
Procedure 54-9 To configure an IGMP policy 54-25
Procedure 54-10 To configure a BGP Peering policy 54-26
Procedure 54-11 To configure a diameter policy 54-29
Procedure 54-12 To configure a subscriber multicast CAC policy 54-31
Procedure 54-13 To configure a mobile gateway profile 54-32
Procedure 54-14 To configure a host lockout policy 54-33
Procedure 54-15 To clear host lockouts 54-34
Procedure 54-16 To configure a RADIUS script policy 54-36
Procedure 54-17 To configure an SLA profile 54-37
Procedure 54-18 To configure a subscriber profile 54-42
Procedure 54-19 To configure a subscriber explicit map 54-48

55 — Remote network monitoring policies 55-1
55.1 Remote network monitoring policies overview 55-2
55.2 Remote network monitoring policies procedures 55-2
Procedure 55-1 To configure a remote network monitoring policy 55-2

56 — Constraint policies 56-1
56.1 Constraint policies overview 56-2
Size constraint policies 56-2
Ageout constraint policies 56-2
56.2 Constraint policies procedures 56-2
Procedure 56-1 To configure a size constraint policy 56-2
Procedure 56-2 To configure an ageout constraint policy 56-3

57 — NAT policies 57-1
57.1 NAT policies overview 57-2

58 — Format and range policies 58-1

58.1 Format and range policies overview 58-2
58.2 Format and range policies procedures 58-5
Procedure 58-1 To create or configure a format policy 58-6
Procedure 58-2 To create or configure a range policy 58-8

59 — PCP policies 59-1

59.1 PCP policies overview 59-2
59.2 Workflow to configure and apply PCP policies 59-2
59.3 PCP policies procedures 59-2
Procedure 59-1 To create a PCP policy 59-2
Procedure 59-2 To view a PCP policy 59-3
Procedure 59-3 To create a NAT PCP server on the base routing instance 59-4
Procedure 59-4 To create a NAT PCP server on a VPRN routing instance 59-4
Procedure 59-5 To associate an interface with a NAT PCP server 59-5
Procedure 59-6 To modify the interface associated with a NAT PCP server 59-6
Procedure 59-7 To modify the routing instance associated with the NAT PCP server 59-7

60 — Firewall policies 60-1

60.1 Overview of firewall policies on the 7705 SAR-H 60-2
Firewall zone management 60-2
60.2 Workflow to configure and manage firewall policies on the 7705 SAR-H 60-4
60.3 Configuring firewall policies for the 7705 SAR-H 60-4
Procedure 60-1 To configure a host group firewall policy 60-4
Procedure 60-2 To configure a service group firewall policy 60-6
Procedure 60-3 To configure a rule set firewall policy 60-9
Procedure 60-4 To configure a zone firewall policy 60-13
Procedure 60-5 To configure a firewall log policy 60-15

Service management

61 — Service management and QoS 61-1

61.1 Service management and QoS overview 61-2
Access interfaces 61-6
Automatic SDP (service tunnel) binding for services 61-7
Multi-segment tunnel selection 61-7
Automatic PBB tunnel binding 61-11
Lightweight SAPs 61-11

61.2 5620 SAM and the triple play service delivery architecture 61-12
Service differentiation and QoS 61-14
BTV multicast 61-19
61.3 BTV multicast configuration examples 61-22
Device preconfiguration 61-22
Network preconfiguration 61-24
Multicast configuration common to all examples 61-25
Example A configuration 61-25
Example B configuration 61-26
Example C configuration 61-26
Example D configuration 61-27
61.4 Sample network configuration using QoS 61-29
61.5 Sample SAP QoS configuration 61-31
61.6 Workflow to implement QoS on an OmniSwitch 61-39
61.7 Workflow to implement QoS on the 7750 SR, 7450 ESS, 7710 SR, 7705 SAR, and 7950 XRS 61-40
61.8 5620 SAM QoS policies 61-41
Access ingress policies 61-44
Access egress policies 61-44
Network policies 61-45
Network queue policies 61-46
Scheduling 61-47
Port scheduler policies 61-47
HSMDA scheduler policies 61-48
Slope policies 61-48
HSMDA slope policies 61-49

62 — Queue groups 62-1

62.1 Queue group overview 62-2
Queue Group Template policies 62-2
Port queue groups 62-2
Port queue group LAGs 62-2
Access SAP forwarding class-based redirection 62-3
Network IP interface forwarding class-based redirection 62-4
Queue group statistics 62-4
Queue group configuration validation rules 62-4
62.2 Workflow to configure access SAP forwarding class-based redirection 62-6
62.3 Workflow to configure network IP interface forwarding class-based redirection 62-7
62.4 Workflow to configure statistics collection for queue groups 62-8

63 — Virtual ports 63-1

63.1 Virtual port overview 63-2
SLA Profiles 63-2
Subscriber Profiles 63-2
63.2 Workflow to configure and manage virtual ports 63-3
63.3 Virtual ports procedures 63-3
Procedure 63-1 To configure a virtual port using the navigation tree 63-3
Procedure 63-2 To configure a virtual port using the Port QoS form 63-4
Procedure 63-3 To copy a virtual port 63-5

64 — Customer configuration and service management 64-1

64.1 Customer configuration and service management overview 64-2
Managing the size of a service associated with a customer 64-2
64.2 Workflow to create a customer profile and manage customer services..... 64-3
64.3 Customer configuration and service management procedures..... 64-3
Procedure 64-1 To create a customer profile..... 64-3
Procedure 64-2 To list the services associated with a customer..... 64-4
Procedure 64-3 To view a service map for a customer..... 64-4
Procedure 64-4 To modify and manage customer information..... 64-5
Procedure 64-5 To move sites from one service to another 64-6
Procedure 64-6 To delete customers..... 64-7

65 — Residential subscriber management 65-1

65.1 Residential subscriber overview 65-2
Residential subscriber components..... 65-2
Subscriber identification strings 65-5
Migrating to the TPSDA model 65-6
65.2 Sample configuration 65-6
65.3 Workflow to manage residential subscribers 65-9
65.4 Residential subscriber management 65-12
Configuration requirements 65-13
Local DHCP server..... 65-13
Local user database..... 65-14
ARP host 65-14
Static hosts and residential subscriber management..... 65-15
Subscriber host connectivity verification..... 65-15
Routed CO 65-17
Subscriber host polling and monitoring 65-19
Subscriber services..... 65-20
Managed routes..... 65-21
65.5 Residential subscriber management procedures 65-22
Procedure 65-1 To enable automatic generation of subscriber IDs..... 65-22
Procedure 65-2 To configure DHCP lease management for a subscriber host..... 65-22
Procedure 65-3 To configure DHCP event monitoring for a subscriber host..... 65-23
Procedure 65-4 To monitor DHCP events for a subscriber host 65-24
Procedure 65-5 To configure a local user database for subscriber host authentication 65-25
Procedure 65-6 To enable or disable subnet draining on a local DHCPv4 server 65-37
Procedure 65-7 To configure NE SHCV event handling 65-38
Procedure 65-8 To retrieve PPPoA sessions 65-39
Procedure 65-9 To configure a MEP on an SDP Binding..... 65-39
Procedure 65-10 To configure L2Aware static port forwarding on a residential subscriber instance..... 65-41
Procedure 65-11 To resynchronize static port forwarding entries..... 65-42
Procedure 65-12 To collect, view, and clear host tracking statistics and information..... 65-43
Procedure 65-13 To view subscriber host information 65-50

Procedure 65-14 To view a subscriber and the associated subscriber hosts 65-51
Procedure 65-15 To view a subscriber instance and its related information 65-52
Procedure 65-16 To view DHCP lease information 65-54
Procedure 65-17 To view SLA policy instances on a subscriber instance 65-55
Procedure 65-18 To view SHCV log events 65-56
Procedure 65-19 To change the identification of a subscriber 65-56
Procedure 65-20 To reset a subscriber's subscription credit limit 65-57
Procedure 65-21 To modify the primary subscriber identification script or URL 65-58
Procedure 65-22 To delete an inactive residential subscriber instance 65-59
65.6 SAP and MSAP management 65-60
SAP DHCP monitoring 65-60
Managed SAP (MSAP) 65-61
65.7 Workflow to manage MSAPs 65-64
65.8 SAP managment procedures 65-65
Procedure 65-23 To manage residential subscriber management components on a SAP 65-65
Procedure 65-24 To enable or disable residential subscriber management on a SAP 65-67
Procedure 65-25 To create a static host for residential subscriber management on a SAP 65-67
Procedure 65-26 To configure a MEP on a SAP 65-70
Procedure 65-27 To list and manage subscriber management SAPs 65-72
Procedure 65-28 To create a capture SAP 65-72
Procedure 65-29 To list MSAPs and view MSAP properties 65-76
Procedure 65-30 To view an MSAP event log, modify the global MSAP log policy, and purge MSAP log records 65-77
Procedure 65-31 To modify and re-evaluate an MSAP policy on an MSAP 65-77
Procedure 65-32 To modify an MSAP policy and re-evaluate the MSAPs 65-78
Procedure 65-33 To re-evaluate lease states for an MSAP 65-79
Procedure 65-34 To delete an MSAP 65-80
Procedure 65-35 To delete an MSAP policy 65-80
Procedure 65-36 To configure DHCP event monitoring for a SAP 65-80
Procedure 65-37 To monitor DHCP events for a SAP 65-81
Procedure 65-38 To view or configure active residential subscriber hosts on a SAP 65-82

66 — VLAN service management 66-1

66.1 VLAN service management overview 66-2
VLAN ring groups 66-2
VLAN groups 66-4
OmniSwitch VLAN service policies 66-4
OmniSwitch network management 66-5
Spanning tree protocols 66-5
66.2 Sample L2 VPN VLAN configuration 66-6

66.3 Sample BTV VLAN configuration 66-8
66.4 Sample interconnection VLAN configuration 66-10
66.5 Workflow to create VLAN services (OmniSwitch) 66-12
66.6 VLAN service management procedures 66-14
Procedure 66-1 To create a standard VLAN service 66-14
Procedure 66-2 To create an OmniSwitch L2 VPN TLS VLAN service 66-17
Procedure 66-3 To create an OmniSwitch BTV VLAN service 66-21
Procedure 66-4 To create an OmniSwitch VIP VLAN service 66-26
Procedure 66-5 To associate an access interface with a VLAN service 66-28
Procedure 66-6 To create a VLAN group 66-29
Procedure 66-7 To delete a VLAN group or group member 66-31
Procedure 66-8 To add a MEP to an OmniSwitch VLAN service access interface 66-31
Procedure 66-9 To configure IGMP on an OmniSwitch VLAN site 66-32
Procedure 66-10 To run an OAM validation test on a VLAN service 66-34
Procedure 66-11 To view the VLAN service operational status 66-35
Procedure 66-12 To view the service topology associated with a VLAN 66-36
Procedure 66-13 To modify a VLAN service 66-36
Procedure 66-14 To delete a VLAN service 66-37

67 — VLL service management 67-1

67.1 VLL service management overview 67-2
VLL types 67-4
VLL spoke switching 67-9
VLL redundancy 67-10
HSDPA Offload Resiliency 67-15
SDP bindings bandwidth allocation 67-17
Port redundancy 67-18
Copying and moving SAPs between ports 67-19
DoS protection 67-19
DDoS protection 67-19
BGP VPWS 67-19
67.2 Sample VLL service 67-19
67.3 Workflow to create a VLL service 67-21
67.4 VLL service management procedures 67-23
Procedure 67-1 To create a VLL Epipe service 67-23
Procedure 67-2 To create a VLL Epipe site 67-25
Procedure 67-3 To link the Epipe service to a backbone VPLS site 67-28
Procedure 67-4 To create a spoke SDP binding on a VLL Epipe site 67-30
Procedure 67-5 To configure an MPLS-TP static pseudowire on an Epipe spoke SDP binding 67-39
Procedure 67-6 To create a spoke SDP FEC binding on a VLL Epipe site 67-40
Procedure 67-7 To configure an Epipe site for BGP multi-homing 67-41
Procedure 67-8 To create a VLL Apipe service 67-44
Procedure 67-9 To create a VLL Apipe site 67-46
Procedure 67-10 To create a spoke SDP binding on a VLL Apipe site 67-47
Procedure 67-11 To configure an MPLS-TP static pseudowire on an Apipe spoke SDP binding 67-51

Procedure 67-12 To create a VLL Fpipe service 67-52
Procedure 67-13 To create a VLL Fpipe site 67-54
Procedure 67-14 To create a spoke SDP binding on a VLL Fpipe site 67-55
Procedure 67-15 To create a VLL Hpipe service 67-59
Procedure 67-16 To create a VLL Hpipe site 67-61
Procedure 67-17 To create a spoke SDP binding on a VLL Hpipe site 67-62
Procedure 67-18 To create a VLL Ipipe service 67-66
Procedure 67-19 To create a VLL Ipipe site 67-68
Procedure 67-20 To create a spoke SDP binding on a VLL Ipipe site 67-70
Procedure 67-21 To create a VLL Cpipe service 67-76
Procedure 67-22 To create a VLL Cpipe site 67-78
Procedure 67-23 To create a spoke SDP binding on a VLL Cpipe site 67-79
Procedure 67-24 To configure an MPLS-TP static pseudowire on an Cpipe spoke SDP binding 67-83
Procedure 67-25 To configure a GNE site on a VLL service 67-84
Procedure 67-26 To create an endpoint for a redundant VLL service.... 67-85
Procedure 67-27 To create a VLL L2 access interface on a terminating site 67-86
Procedure 67-28 To assign ingress and egress QoS policies to a VLL L2 access interface 67-94
Procedure 67-29 To configure scheduling on a VLL L2 access interface 67-97
Procedure 67-30 To assign ingress and egress ACL filters to the VLL L2 access interface 67-100
Procedure 67-31 To assign an accounting policy to a VLL L2 access interface 67-102
Procedure 67-32 To assign a time of day suite to the VLL L2 access interface 67-103
Procedure 67-33 To assign a DoS protection policy or DDoS protection policy to an Epipe or Ipipe L2 access interface 67-104
Procedure 67-34 To associate a MEP with an Epipe or Apipe L2 access interface 67-104
Procedure 67-35 To configure microwave compression on an MW link SAP associated with a 7705 SAR on the VLL L2 access interface 67-108
Procedure 67-36 To configure an Ethernet tunnel on a VLL L2 access interface 67-109
Procedure 67-37 To assign an ANCP policy to a VLL L2 access interface 67-110
Procedure 67-38 To specify OAM functionality and assign ingress and egress ATM policies an Epipe, Apipe, or Ipipe L2 access interface 67-110
Procedure 67-39 To specify the CEM functionality for an Epipe L2 access interface with CEM encapsulation 67-112
Procedure 67-40 To specify the CEM functionality for the Cpipe L2 access interface..... 67-113
Procedure 67-41 To switch to the redundant port for a VLL SAP from an L2 access interface properties form 67-114
Procedure 67-42 To switch to the redundant port for one or more VLL SAPs from a service, site, or port properties form 67-115
Procedure 67-43 To create a SAP aggregation group 67-118
Procedure 67-44 To create an HSDPA resiliency configuration 67-120

Procedure 67-45 To activate and manually operate an HSDPA resiliency configuration 67-121
Procedure 67-46 To run an OAM validation test for a VLL service 67-122
Procedure 67-47 To view the service topology associated with a VLL service 67-123
Procedure 67-48 To view the VLL service operational status 67-124
Procedure 67-49 To view the local PW status information for a VLL service 67-124
Procedure 67-50 To view the peer PW status information for a VLL service 67-125
Procedure 67-51 To modify a VLL service 67-125
Procedure 67-52 To modify a VLL service using the topology view 67-126
Procedure 67-53 To delete a VLL service 67-129
Procedure 67-54 To create a BGP VPWS 67-130

68 — VPLS management 68-1

68.1 VPLS management overview 68-2
HVPLS 68-4
MVPLS 68-5
Dual homing for VPLS 68-7
Provider Backbone Bridging in VPLS 68-9
SPB in VPLS 68-14
BGP Auto Discovery 68-16
BGP VPLS 68-17
BGP VPLS Multi-homing 68-18
MVR on VPLS 68-19
GSMP group on VPLS 68-21
L2 management interfaces on VPLS 68-22
Routed VPLS 68-22
FIBs 68-22
MAC learning 68-23
MAC move 68-24
Flooding 68-24
Spanning tree protocols 68-25
IGMP snooping 68-25
MLD snooping 68-26
PIM snooping 68-26
Split horizon groups 68-27
Residential split horizon groups 68-27
Default SAPs 68-28
Layer 2 protocol tunneling termination 68-29
BPDU translation 68-30
DoS protection 68-30
DDoS protection 68-30
Copying and moving SAPs between ports 68-30
68.2 Sample VPLS configuration 68-30
68.3 Workflow to create a VPLS 68-37
68.4 VPLS management procedures 68-41
Procedure 68-1 To create a VPLS 68-41
Procedure 68-2 To configure a VPLS for AA reporting to the 5670 RAM 68-42

Procedure 68-3 To assign a multicast package policy to a VPLS 68-43
Procedure 68-4 To configure bandwidth management for a VPLS..... 68-44
Procedure 68-5 To configure the VPLS for BGP auto-discovery 68-45
Procedure 68-6 To add protected MAC addresses to a VPLS..... 68-46
Procedure 68-7 To configure a VPLS site 68-46
Procedure 68-8 To configure MFIB, STP, FIB, and MAC learning protection for a VPLS site..... 68-50
Procedure 68-9 To configure SHCV for a VPLS site..... 68-53
Procedure 68-10 To configure a default gateway for a VPLS site..... 68-53
Procedure 68-11 To configure ingress multicast forwarding on a VPLS site 68-54
Procedure 68-12 To configure a provider tunnel for a VPLS site 68-55
Procedure 68-13 To configure service tunnel required bandwidth for a VPLS site 68-56
Procedure 68-14 To configure IGMP snooping on a VPLS site..... 68-57
Procedure 68-15 To create an endpoint for redundancy (dual homing) on a VPLS site 68-58
Procedure 68-16 To configure an SHG on a VPLS site 68-59
Procedure 68-17 To configure MVR for a VPLS site 68-60
Procedure 68-18 To configure a GSMP group on a VPLS site..... 68-61
Procedure 68-19 To configure L2 management interfaces on a VPLS site 68-62
Procedure 68-20 To configure MLD snooping for a VPLS site 68-63
Procedure 68-21 To create a virtual MEP on a VPLS site..... 68-64
Procedure 68-22 To configure MVR for MLD on a VPLS site 68-65
Procedure 68-23 To configure IGMP host tracking on a VPLS site 68-66
Procedure 68-24 To create a VPLS or MVPLS L2 access interface 68-67
Procedure 68-25 To assign ingress and egress QoS policies to an L2 access interface..... 68-76
Procedure 68-26 To configure scheduling on an L2 access interface 68-79
Procedure 68-27 To configure BPDU Termination, STP, and FIB parameters for the VPLS L2 access interface 68-83
Procedure 68-28 To assign a DoS protection policy or DDoS protection policy to the VPLS L2 access interface 68-85
Procedure 68-29 To configure residential subscriber management for the VPLS L2 access interface..... 68-86
Procedure 68-30 To configure an Ethernet tunnel on a VPLS L2 access interface 68-88
Procedure 68-31 To configure a redundant VLAN range on a VPLS L2 access interface..... 68-89
Procedure 68-32 To configure IGMP snooping for the VPLS L2 access interface 68-90
Procedure 68-33 To configure the ARP host for the VPLS L2 access interface 68-92
Procedure 68-34 To configure DHCP for the VPLS L2 access interface..... 68-93
Procedure 68-35 To configure MVR for a VPLS L2 access interface 68-95
Procedure 68-36 To configure anti-spoofing filters for a VPLS L2 access interface 68-96
Procedure 68-37 To associate a MEP with a VPLS L2 access interface... 68-98
Procedure 68-38 To assign an ANCP policy to a VPLS L2 access interface..... 68-102

Procedure 68-39 To configure PIM snooping on a VPLS L2 access interface 68-103
Procedure 68-40 To configure MLD snooping for a VPLS L2 access interface 68-103
Procedure 68-41 To configure MVR (MLD) for a VPLS L2 access interface 68-105
Procedure 68-42 To configure custom object attributes for AA reporting to the 5670 RAM 68-106
Procedure 68-43 To create a VPLS mesh SDP binding 68-107
Procedure 68-44 To create a VPLS spoke SDP binding 68-113
Procedure 68-45 To configure an MPLS-TP static pseudowire on a VPLS spoke SDP binding 68-121
Procedure 68-46 To assign a DoS protection policy to a VPLS SDP binding 68-122
Procedure 68-47 To configure MFIB, STP, FIB, MRP, and MAC learning protection parameters on a VPLS SDP binding 68-123
Procedure 68-48 To configure DHCP for the VPLS SDP binding 68-125
Procedure 68-49 To configure IGMP snooping for the VPLS SDP binding 68-126
Procedure 68-50 To associate a MEP with the VPLS SDP binding 68-128
Procedure 68-51 To configure MLD Snooping for the VPLS SDP binding 68-130
Procedure 68-52 To configure PIM snooping for the VPLS SDP binding 68-131
Procedure 68-53 To configure custom object attributes for AA reporting to the 5670 RAM for a spoke SDP binding 68-132
Procedure 68-54 To configure a site for BGP AD or BGP VPLS 68-133
Procedure 68-55 To configure a site for BGP VPLS Multi-homing 68-138
Procedure 68-56 To re-evaluate the PW Templates associated with a BGP AD or BGP VPLS 68-142
Procedure 68-57 To assign tunnel administrative groups to a BGP or BGP AD VPLS 68-143
Procedure 68-58 To create an HVPLS 68-144
Procedure 68-59 To create an MVPLS 68-145
Procedure 68-60 To create a B-site for VPLS or MVPLS 68-148
Procedure 68-61 To enable SPB on a control B-VPLS site 68-155
Procedure 68-62 To enable SPB on a user B-VPLS site 68-158
Procedure 68-63 To view SPB fate-shared objects 68-159
Procedure 68-64 To view SPB instances on an NE 68-160
Procedure 68-65 To create an I-VPLS 68-160
Procedure 68-66 To create a VPLS or MVPLS B-L2 access interface 68-168
Procedure 68-67 To create a static ISID range on a VPLS B-L2 access interface or spoke SDP binding 68-178
Procedure 68-68 To create a static B-MAC on a B-VPLS site 68-179
Procedure 68-69 To create an ISID policy on a control or user B-VPLS site 68-180
Procedure 68-70 To create a VPLS I-L2 access interface 68-181
Procedure 68-71 To configure a GNE site on a VPLS service 68-194
Procedure 68-72 To force a switchover to a redundant spoke SDP binding 68-196
Procedure 68-73 To run a VPLS service OAM validation test 68-196

Procedure 68-74 To add or modify FIB entries associated with a VPLS 68-197
Procedure 68-75 To list FIB entries associated with a VPLS 68-198
Procedure 68-76 To view the service topology associated with a VPLS service 68-199
Procedure 68-77 To view the VPLS service operational status 68-199
Procedure 68-78 To view IGMP snooping queriers 68-200
Procedure 68-79 To view MLD snooping queriers 68-201
Procedure 68-80 To modify a VPLS 68-201
Procedure 68-81 To modify a VLPS using the topology view 68-203
Procedure 68-82 To delete a VPLS 68-209

69 — Mirror service management 69-1

69.1 Mirror service overview 69-2
69.2 Sample mirror service configuration 69-4
69.3 Workflow to create a mirror service 69-5
69.4 Mirror service procedures 69-7
Procedure 69-1 To create a mirror service 69-7
Procedure 69-2 To create a destination site on a mirror service 69-9
Procedure 69-3 To create a source site on a mirror service 69-11
Procedure 69-4 To configure an MPLS-TP static pseudowire on a mirror SDP binding 69-15
Procedure 69-5 To create an endpoint for redundancy support on the site 69-16
Procedure 69-6 To create an L2 access interface on a destination site 69-18
Procedure 69-7 To specify a SAP on the site as a mirror source 69-21
Procedure 69-8 To specify a port on the site as a mirror source 69-22
Procedure 69-9 To specify a source IP or LI source IP filter entry for the mirror source 69-23
Procedure 69-10 To specify a source IPv6 or LI source IPv6 filter entry for the mirror source 69-24
Procedure 69-11 To specify a source MAC or LI source MAC filter entry for the mirror site 69-26
Procedure 69-12 To specify an LI source LI MAC filter for the mirror site 69-27
Procedure 69-13 To specify an MPLS ingress label for the mirror 69-28
Procedure 69-14 To specify a source subscriber or LI source subscriber as a mirror source 69-28
Procedure 69-15 To view the service topology associated with a mirror service 69-30
Procedure 69-16 To view the mirror service operational status 69-31
Procedure 69-17 To view LI mirrored subscriber hosts configured with a RADIUS server 69-31
Procedure 69-18 To create a mirror port on a 7210 SAS 69-32
Procedure 69-19 To run an OAM validation test for a mirror service 69-33
Procedure 69-20 To modify a mirror service 69-34
Procedure 69-21 To delete a mirror service 69-34

70 — IES management 70-1

70.1 IES management overview 70-2
IES configuration 70-2
ATM SAP terminations for IES 70-4
Routed CO dual homing using SRRP 70-5
DoS protection 70-7
DDoS protection 70-7
Local DHCP servers 70-7
Local user database 70-8
PPPoE protocol on IES 70-8
L2TP configuration for IES 70-8
70.2 Sample IES configuration 70-8
70.3 Workflow to create an IES 70-10
70.4 IES management procedures 70-13
Procedure 70-1 To create an IES 70-13
Procedure 70-2 To configure an IES for AA reporting to the 5670 RAM 70-14
Procedure 70-3 To configure an IES site 70-15
Procedure 70-4 To configure a GNE site on an IES service 70-16
Procedure 70-5 To apply OSPF, RIP, or IS-IS to an IES site 70-17
Procedure 70-6 To add an IGMP interface to an IES 70-18
Procedure 70-7 To add a PIM interface to an IES 70-21
Procedure 70-8 To create an L2 SDP spoke termination on an IES service 70-23
Procedure 70-9 To configure an MPLS-TP static pseudowire on an IES spoke SDP binding 70-28
Procedure 70-10 To configure a subscriber interface on an IES 70-29
Procedure 70-11 To add an AARP interface to an IES 70-33
Procedure 70-12 To configure a group interface on an IES 70-34
Procedure 70-13 To configure a WLAN GW for an IES group interface 70-53
Procedure 70-14 To add a TMS interface to an IES 70-56
Procedure 70-15 To implement dual homing using SRRP 70-59
Procedure 70-16 To configure IGMP host tracking on an IES site 70-62
Procedure 70-17 To configure an L3 access interface on an IES site 70-63
Procedure 70-18 To configure custom object attributes for AA reporting to the 5670 RAM on an IES L3 access interface 70-66
Procedure 70-19 To bind an IES L3 access interface to a VPLS site or VPLS I-site 70-67
Procedure 70-20 To apply OSPF, RIP, or IS-IS to an IES L3 interface 70-68
Procedure 70-21 To assign ingress and egress QoS policies to an IES L3 access interface 70-69
Procedure 70-22 To assign ingress and egress QoS policies to an IES L3 access interface on the 7210 SAS 70-72
Procedure 70-23 To configure scheduling on an IES L3 access interface 70-73
Procedure 70-24 To assign ingress and egress ACL filters to an IES L3 access interface 70-75
Procedure 70-25 To associate a local DHCPv4 or DHCPv6 server to an IES L3 access interface 70-76
Procedure 70-26 To assign an accounting policy to an IES L3 access interface 70-77

Procedure 70-27 To assign an ANCP policy to an IES L3 access interface 70-78
Procedure 70-28 To assign a time of day suite to an IES L3 access interface 70-79
Procedure 70-29 To configure residential subscriber management for an IES L3 access interface 70-80
Procedure 70-30 To assign a DoS protection policy or DDoS protection policy to an IES L3 access interface 70-81
Procedure 70-31 To assign an IP address to an IES L3 access interface 70-81
Procedure 70-32 To configure bi-directional forwarding detection for an IES L3 access interface 70-82
Procedure 70-33 To configure IPv4 ICMP for an IES L3 access interface 70-83
Procedure 70-34 To configure IPv6 ICMP on an IES L3 access interface 70-84
Procedure 70-35 To configure IPCP for an IES L3 access interface 70-85
Procedure 70-36 To configure ARP for an IES L3 access interface 70-86
Procedure 70-37 To configure neighbor discovery on an IES L3 access interface 70-87
Procedure 70-38 To configure IPv4 DHCP for an IES L3 access interface 70-88
Procedure 70-39 To configure ATM on an IES L3 access interface 70-90
Procedure 70-40 To create a VRRP instance on an IES L3 access interface for a virtual router 70-91
Procedure 70-41 To configure anti-spoofing filters for an IES L3 access interface 70-92
Procedure 70-42 To configure router advertisement on an IES L3 access interface 70-93
Procedure 70-43 To specify queue overrides on an IES L3 access interface 70-95
Procedure 70-44 To configure IPv6 DHCP on an IES L3 access interface 70-95
Procedure 70-45 To view the service operational status 70-97
Procedure 70-46 To view the service topology 70-97
Procedure 70-47 To modify an IES 70-98
Procedure 70-48 To modify an IES using the topology view 70-99
Procedure 70-49 To delete an IES 70-101

71 — VPRN service management 71-1

71.1 VPRN service management overview 71-2
VPRN service routers 71-4
Inter-AS connections 71-5
MP-BGP Multicast IPv4 71-6
IPv6 support 71-6
PIM for VPRN 71-6
OSPF sham link support 71-7
ATM SAP terminations for VPRN 71-8
Epipe SDP spoke termination on VPRN services 71-9
Routed CO dual homing using SRRP 71-10
DoS protection 71-11

DDoS protection 71-11
Local DHCP servers..... 71-12
Local user database..... 71-12
PPPoE protocol on VPRN services..... 71-12
L2TP on VPRN services 71-13
IPsec..... 71-13
71.2 Sample VPRN service configuration 71-13
71.3 Sample hub-and-spoke VPRN configuration 71-16
71.4 Workflow to create a VPRN service 71-20
71.5 VPRN service management procedures 71-22
Procedure 71-1 To create a VPRN service 71-22
Procedure 71-2 To configure AA reporting to the 5670 RAM 71-23
Procedure 71-3 To configure a VPRN site..... 71-23
Procedure 71-4 To configure an SNMP community for mediating the IPv6 objects on a VPRN site..... 71-25
Procedure 71-5 To configure an MVPN VRF instance on a VPRN site 71-26
Procedure 71-6 To enable routing protocols on a VPRN site 71-30
Procedure 71-7 To resync soft GRE tunnels on a VPRN site 71-31
Procedure 71-8 To configure a BGP confederation on a VPRN site 71-32
Procedure 71-9 To configure a routing instance on a VPRN site 71-33
Procedure 71-10 To bind a VPRN site to service tunnels..... 71-39
Procedure 71-11 To configure VRF import and export policies on a VPRN site 71-41
Procedure 71-12 To configure static routes on a VPRN site 71-42
Procedure 71-13 To configure a GSMP group on a VPRN site 71-43
Procedure 71-14 To configure a local DHCPv4 server on a VPRN site 71-45
Procedure 71-15 To configure a local DHCPv6 server on a VPRN site 71-45
Procedure 71-16 To configure DSCP on a VPRN site 71-46
Procedure 71-17 To configure an override source IP address or L3 interface on a VPRN site 71-47
Procedure 71-18 To configure IGMP host tracking on a VPRN site..... 71-48
Procedure 71-19 To configure WLAN gateway functionality on a VPRN site 71-49
Procedure 71-20 To configure DNS for a VPRN site 71-50
Procedure 71-21 To configure route aggregates on a VPRN site 71-50
Procedure 71-22 To configure an L3 access interface on a VPRN site ... 71-51
Procedure 71-23 To configure NTP on a VPRN site..... 71-56
Procedure 71-24 To configure custom object attributes for AA reporting to the 5670 RAM on a VPRN L3 access interface 71-57
Procedure 71-25 To assign ingress and egress QoS policies to a VPRN L3 access interface 71-58
Procedure 71-26 To configure scheduling on a VPRN L3 access interface..... 71-61
Procedure 71-27 To assign ingress and egress ACL filters to a VPRN L3 access interface 71-64
Procedure 71-28 To assign an accounting policy to a VPRN L3 access interface 71-65
Procedure 71-29 To assign a time of day suite to a VPRN L3 access interface 71-66
Procedure 71-30 To bind a VPRN L3 access interface to a VPLS site or VPLS I-site..... 71-67

Procedure 71-31 To associate a local DHCPv4 or DHCPv6 server with a VPRN L3 access interface 71-68
Procedure 71-32 To assign an NE DoS protection policy or NE DDoS protection policy to a VPRN L3 access interface 71-70
Procedure 71-33 To configure residential subscriber management for a VPRN L3 access interface 71-70
Procedure 71-34 To assign an IP address to a VPRN L3 access interface 71-71
Procedure 71-35 To configure IPv4 ICMP for a VPRN L3 access interface 71-72
Procedure 71-36 To configure IPv6 ICMP on a VPRN L3 access interface 71-73
Procedure 71-37 To configure IPCP for a VPRN L3 access interface 71-74
Procedure 71-38 To configure Bi-directional Forwarding Detection for a VPRN L3 access interface 71-75
Procedure 71-39 To configure ARP for a VPRN L3 access interface 71-76
Procedure 71-40 To configure neighbor discovery on a VPRN L3 access interface 71-77
Procedure 71-41 To configure IPv4 DHCP for a VPRN L3 access interface 71-78
Procedure 71-42 To create a VRRP instance on a VPRN L3 access interface for a virtual router 71-80
Procedure 71-43 To configure anti-spoofing filters for a VPRN L3 access interface 71-81
Procedure 71-44 To configure router advertisement on a VPRN L3 access interface 71-83
Procedure 71-45 To assign an ANCP policy to a VPRN L3 access interface 71-84
Procedure 71-46 To specify queue overrides on a VPRN L3 access interface 71-85
Procedure 71-47 To configure IPv6 DHCP on a VPRN L3 access interface 71-86
Procedure 71-48 To configure a VPRN network interface 71-87
Procedure 71-49 To configure a GNE site on a VPRN service 71-93
Procedure 71-50 To configure OSPFv2, OSPFv3, PIM, RIP, L2TP, or MLD on a VPRN routing instance 71-95
Procedure 71-51 To configure BGP on a VPRN routing instance 71-96
Procedure 71-52 To configure IGMP on a VPRN routing instance 71-101
Procedure 71-53 To add a Global Route Table to a VPRN site 71-103
Procedure 71-54 To add a PIM interface to a VPRN 71-104
Procedure 71-55 To add an IGMP interface to a VPRN 71-105
Procedure 71-56 To create a VPRN spoke SDP binding 71-107
Procedure 71-57 To create an L2 SDP spoke termination on a VPRN service 71-113
Procedure 71-58 To configure an MPLS-TP static pseudowire on a VPRN spoke SDP binding 71-117
Procedure 71-59 To configure a subscriber interface on a VPRN 71-118
Procedure 71-60 To configure a group interface on a VPRN 71-123
Procedure 71-61 To collect and view PPP ATM SAP statistics and information for a VPRN group interface 71-140
Procedure 71-62 To configure a WLAN GW for a VPRN group interface 71-141

Procedure 71-63 To add an IP mirror interface to a VPRN 71-144
Procedure 71-64 To add a TMS interface to a VPRN 71-145
Procedure 71-65 To implement dual homing using SRRP 71-147
Procedure 71-66 To create an OSPF sham link 71-151
Procedure 71-67 To run an OAM validation test for a VPRN service 71-153
Procedure 71-68 To view the service topology map associated with a VPRN service 71-154
Procedure 71-69 To view the VPRN service operational status 71-154
Procedure 71-70 To view DHCPv6 leases 71-155
Procedure 71-71 To view DHCPv6 log events 71-156
Procedure 71-72 To modify a VPRN service 71-157
Procedure 71-73 To modify a VPRN service using the topology view ... 71-158
Procedure 71-74 To delete a VPRN service 71-162

72 — PW routing and dynamic MS-PW service management 72-1

72.1 PW routing and dynamic MS-PW service management overview 72-2
PW routing 72-2
MS-PW routing 72-2
Dynamic MP-PW services 72-3
72.2 Workflow to configure PW routing and dynamic MS-PW services 72-3
72.3 PW routing and dynamic MS-PW service management procedures 72-5
Procedure 72-1 To configure PW routing using the navigation tree 72-5
Procedure 72-2 To create, modify, or view a PW routing NE configuration using the Manage Services form 72-7
Procedure 72-3 To configure a dynamic MS-PW service using PW routing 72-9
Procedure 72-4 To display MS-PW routing tables 72-11
Procedure 72-5 To perform spoke SDP FEC operations from an endpoint 72-12
Procedure 72-6 To discover and manage MS-PW switching sites 72-12
Procedure 72-7 To conduct MS-PW routing OAM tests 72-13

73 — Service PW template policy management 73-1

73.1 Service PW template policies overview 73-2
73.2 Workflow to configure PW template policies 73-2
73.3 Service PW template policies procedures 73-2
Procedure 73-1 To create a PW template policy 73-2
Procedure 73-2 To distribute a PW template policy 73-5
Procedure 73-3 To reevaluate a PW template policy on a local definition after a configuration change 73-6

74 — Composite service management 74-1

74.1 Composite service management overview 74-2
Hierarchical organization of composite services 74-3
Network discovery of composite services 74-4
Connector types 74-5
74.2 Sample composite service configuration 74-7
74.3 Workflow to create a composite service 74-8

74.4 Composite service management procedures 74-9
Procedure 74-1 To create a composite service 74-10
Procedure 74-2 To add services to a composite service 74-10
Procedure 74-3 To create a cross connect connector 74-11
Procedure 74-4 To create an SCP connector 74-13
Procedure 74-5 To create a spoke connector 74-14
Procedure 74-6 To create a routed VPLS connector 74-16
Procedure 74-7 To run an OAM validation test for a composite service 74-18
Procedure 74-8 To rediscover composite services 74-19
Procedure 74-9 To view the service topology map associated with a composite service 74-19
Procedure 74-10 To modify a composite service using the navigation tree 74-20
Procedure 74-11 To modify a composite service using the flat topology view 74-21
Procedure 74-12 To delete a composite service 74-25

75 — Dynamic service management 75-1

75.1 Dynamic service management overview 75-2
Dynamic service structure 75-2
75.2 Dynamically-created objects 75-3
Unsupported operations 75-3
ID range behavior 75-3
75.3 Workflow to create dynamic services 75-4
75.4 Dynamic service management procedures 75-4
Procedure 75-1 To configure a dynamic service policy 75-5
Procedure 75-2 To configure an NE for dynamic service 75-6
Procedure 75-3 To list dynamically created objects on an NE 75-6

76 — Application assurance 76-1

76.1 Application assurance overview 76-2
AA protocol signatures 76-3
AA policers 76-3
AA flow watermark policies 76-4
AA transit IP and transit prefix policies 76-4
Application performance reporting 76-4
AA HTTP error redirect policies 76-4
76.2 ISA-AA groups and partitions 76-4
Multiple ISA-AA groups 76-5
ISA-AA partitions 76-5
76.3 AA components 76-6
AA group policies 76-7
Applications 76-8
Application groups 76-8
Application profiles 76-8
Application filters 76-10
AQPs 76-10
Custom protocols 76-11

76.4 5670 RAM reporting attributes 76-11
Usage-based billing 76-12
Residential DCP groups 76-12
76.5 AA accounting policies 76-13
76.6 Workflow to configure AA 76-14
76.7 Application assurance procedures 76-15
Procedure 76-1 To configure an AA group policy 76-16
Procedure 76-2 To configure AARP 76-23
Procedure 76-3 To configure an AA policer 76-25
Procedure 76-4 To renumber application filter entries 76-27
Procedure 76-5 To configure an AQP 76-28
Procedure 76-6 To configure a policy sync group 76-32
Procedure 76-7 To configure an AA accounting policy 76-35
Procedure 76-8 To configure an AA flow watermark 76-36
Procedure 76-9 To configure an AA transit IP policy 76-37
Procedure 76-10 To configure an AA transit prefix policy 76-39
Procedure 76-11 To configure a database persisted transit subscriber aggregator 76-41
Procedure 76-12 To associate a database persisted transit subscriber with an aggregator 76-42
Procedure 76-13 To configure 5670 RAM AA reporting attributes for a database persisted transit subscriber 76-42
Procedure 76-14 To view database persisted transit subscriber information 76-43
Procedure 76-15 To configure usage-based billing for an application profile 76-44
Procedure 76-16 To associate an application with a charging group 76-45
Procedure 76-17 To enable application performance reporting on a service using default DCP subnet groups 76-46
Procedure 76-18 To disable application performance reporting on a service 76-47
Procedure 76-19 To configure a custom DCP subnet group 76-48
Procedure 76-20 To configure an AA HTTP error redirect policy 76-50
Procedure 76-21 To configure an AA HTTP redirect policy 76-51
Procedure 76-22 To configure an AA HTTP enrichment policy 76-52
Procedure 76-23 To configure an HTTP notification policy 76-54
Procedure 76-24 To configure an AA session filter 76-55
Procedure 76-25 To configure a URL filter 76-57
Procedure 76-26 To enable an AA protocol signature 76-58
Procedure 76-27 To view AA summary information for an ISA-AA group or partition 76-58
Procedure 76-28 To view AA statistics data for an ISA-AA group or partition 76-60
Procedure 76-29 To view the AA special study statistics data 76-61
Procedure 76-30 To view AA statistics data for application filters 76-62
Procedure 76-31 To delete an AA application, application group, or custom protocol 76-63
Procedure 76-32 To delete an inactive AA transit subscriber instance 76-64

77 — Service Test Manager 77-1

77.1 Service Test Manager overview 77-2
Test policies 77-2
Test suites 77-2
77.2 Sample Service Test Manager implementation 77-4
77.3 Sample network monitoring configuration 77-7
77.4 Sample network monitoring configuration steps 77-8
77.5 Sample SAA accounting files configuration 77-14
77.6 Sample SAA accounting files configuration steps 77-14
77.7 Sample threshold-crossing alarm configuration 77-16
77.8 Sample threshold-crossing alarm configuration steps 77-17
77.9 7210 SAS Y.1564 service test 77-19
Workflow to configure and execute Y.1564 bidirectional tests 77-20
77.10 Sample 7210 SAS Y.1564 service test configuration steps 77-20
77.11 Sample OmniSwitch device SLA testing 77-26
77.12 Workflow to use the Service Test Manager 77-31
77.13 Service Test Manager procedures 77-33
Procedure 77-1 To configure a STM test policy 77-33
Procedure 77-2 To configure threshold-crossing alarms on NE-schedulable OAM tests within a test policy 77-43
Procedure 77-3 To configure threshold-crossing alarms on non-NE-schedulable OAM tests within a test policy 77-45
Procedure 77-4 To create a test suite 77-46
Procedure 77-5 To modify a test suite 77-50
Procedure 77-6 To schedule the execution of a test suite 77-52
Procedure 77-7 To schedule the execution of a test suite using an existing NE schedule 77-53
Procedure 77-8 To execute a STM test suite 77-53
Procedure 77-9 To run a One Time Validation 77-54
Procedure 77-10 To execute one or more individual tests from the STM 77-56
Procedure 77-11 To view Test Suite results 77-57
Procedure 77-12 To view and compare Test Suite results for a tested entity 77-58
Procedure 77-13 To view and compare test results 77-58
Procedure 77-14 To delete a test suite 77-59

78 — Ethernet CFM 78-1

78.1 Ethernet CFM overview 78-2
MEGs 78-2
MEPs 78-2
MIPs 78-5
Ethernet-CFM redundancy 78-5
Sample Ethernet CFM implementation 78-5
Ethernet CFM implementation for composite services 78-6
Primary VLAN support for Ethernet CFM 78-9
78.2 Workflow to configure Ethernet CFM 78-11
78.3 Ethernet CFM procedures 78-12
Procedure 78-1 To configure an Ethernet CFM MD and subordinate objects associated with the MD 78-12
Procedure 78-2 To configure automatic MEP ID assignment on an NE ... 78-27

Procedure 78-3 To automatically create identical MEPs on a redundant pair of service SAPs 78-27
Procedure 78-4 To change the MEG sub-group association for managed MEPs or unmanaged remote MEPs 78-29
Procedure 78-5 To configure a default MD on an OmniSwitch 78-30

79 — Tunnel administrative groups 79-1

79.1 Tunnel administrative groups overview 79-2
79.2 Workflow to configure tunnel administrative groups 79-3
79.3 Tunnel administrative group procedures 79-3
Procedure 79-1 To create a tunnel administrative group 79-3
Procedure 79-2 To list and view tunnel administrative groups 79-4

80 — RCA audit 80-1

80.1 RCA audit overview 80-2
5620 SAM service audit 80-2
Physical link audits 80-4
Viewing and analyzing RCA audit results 80-5
80.2 Workflow to configure RCA audit 80-8
80.3 RCA audit procedures 80-9
Procedure 80-1 To configure an RCA audit policy 80-9
Procedure 80-2 To perform an RCA audit of a VLL service 80-11
Procedure 80-3 To perform an RCA audit of a VPLS 80-13
Procedure 80-4 To perform an RCA audit of a VPRN service 80-15
Procedure 80-5 To perform an RCA audit of multiple services 80-17
Procedure 80-6 To perform an RCA audit of a physical link 80-19
Procedure 80-7 To create a service audit scheduled task 80-20

81 — Service throughput configuration 81-1

81.1 Service throughput configuration overview 81-2
81.2 Workflow to prepare for and restore from a service throughput configuration 81-2
81.3 Service throughput configuration procedures 81-3
Procedure 81-1 To prepare a service throughput configuration 81-3
Procedure 81-2 To restore a service after a throughput configuration 81-7

Getting started

1 — What's new?

2 — 5620 SAM system overview

3 — 5620 SAM GUI overview

4 — 5620 SAM custom workspaces

5 — 5620 SAM navigation tree overview

6 — 5620 SAM topology map management

7 — 5620 SAM scheduling

1 — What's new?

1.1 What's new in 5620 SAM Release 11.0 *1-2*

1.1 What's new in 5620 SAM Release 11.0

This section highlights new features for 5620 SAM Release 11.0 and provides pointers into the documentation for more information.

New features and enhancements for this release are also described in the following guides:

- *5620 SAM XML OSS Interface Developer Guide*
- *5620 SAM LTE OSS Interface Developer Guide*
- *5620 SAM LTE EPC User Guide*
- *5620 SAM LTE RAN User Guide*
- *5620 SAM Optical User Guide*
- *5620 SAM MPR User Guide*
- *5650 CPAM User Guide*

The *5620 SAM Release Description* and *5620 SAM LTE Release Description* provide Committed and Candidate feature lists for the entire 11.0 Release. The release description documents not only include the NMS features and nodal features that are documented in 5620 SAM customer documentation, they also identify the nodal features supported by the 5620 SAM but documented in the NE customer documentation.

What's new in 5620 SAM Release 11.0 R8

Table 1-1 lists the features added in 5620 SAM Release 11.0 R8 and described in 5620 SAM core customer documentation.

Table 1-1 5620 SAM Release 11.0 R8 features

Feature ID	Feature or function	Description	See
7450 ESS and 7750 SR enhancements			
SAM-33075 SAM-33077 SAM-33079	New card support	The 5620 SAM supports provisioning the following cards on the 7750 SR-12E: • 2Tb CPM / Switch Fabric 5 E • M-SFM5-12E	Chapter 15
SAM-40903 SAM-40905	CPM5 and SFM5 support	The 5620 SAM supports the discovery of CPM5 and SFM5 modules in 7450 ESS and 7750 SR nodes. CPM5 modules are removable and are displayed as a separate node in the Equipment tree.	—

What's new in 5620 SAM Release 11.0 R7

Table 1-2 lists the features added in 5620 SAM Release 11.0 R7 and described in 5620 SAM core customer documentation.

Table 1-2 5620 SAM Release 11.0 R7 features

Feature ID	Feature or function	Description	See
Device management enhancements			
SAM-26607	Stable pool sizing	The 5620 SAM now supports the configuring of stable pool sizing on FP2 MDAs to enable an even split of buffering.	Procedure 15-29
7210 SAS-T enhancements			
SAM-31356	SyncE support	The 5620 SAM supports Synchronous Ethernet timing synchronization for the 7210 SAS-T and 7210 SAS-T ETR, Release 6.0 R3.	Procedure 15-7
SAM-31356	PoE support on the 7210 SAS-T ETR	The 5620 SAM supports Power over Ethernet on the 7210 SAS-T ETR, Release 6.0 R3.	Procedure 16-18
7705 SAR enhancements			
SAM-20723	10-port 1GigE/1-port 10GigE X-Adapter card with encryption	The 5620 SAM supports the 10-port 1GigE/1-port 10GigE X-Adapter card with encryption, on the 7705 SAR-18, Release 6.0 R5 or later.	Section 8.9
SAM-20725	8-port GigE SFP card with encryption	The 5620 SAM supports the 8-port GigE SFP card with encryption, on the 7705 SAR-8 and the 7705 SAR-18, Release 6.0 R5 or later.	Section 8.9
SAM-20729	6-port FXS Adapter card	The 5620 SAM supports the 6-port FXS Adapter card, on the 7705 SAR-8 and 7705 SAR-18, Release 6.0 R5 or later.	Section 8.9
SAM-30549	Peer discovery	The 5620 SAM supports the option to disable peer discovery on a microwave link on the 7705 SAR-8 and 7705 SAR-18, Release 6.0 R5 or later.	Procedure 15-11
7950 XRS enhancements			
SAM-30098	Power management	The 5620 SAM supports configuring power management zones on 7950 XRS nodes, and power priority values on MDAs installed in 7950 XRS nodes. Detailed information about power usage is available on the power management zone, shelf, card slot, and daughter card slot configuration forms for 7950 XRS nodes.	Section 15.2 Procedure 15-21 Procedure 15-22 Procedure 15-33
Network management enhancements			
SAM-27518	RFE 147695: certificate authentication fails between SR and eNodeB (SHA-2 support for certificate signature)	The 5620 SAM supports the following signature algorithms for local certificate generation requests: • SHA-1 • SHA-256 • SHA-224 • SHA-384 • SHA-512	*5620 SAM System Administrator Guide*
SAM-30604	GNE management client cross-launch from navigation tree	You can enable a network navigation tree contextual menu option that opens an alternate EMS client application for a GNE.	Section 9.2 Procedures 9-7 and 9-8
SAM-31119	High limit for IP next hops	Configurable IP next hop entry limit for hosts' managed routes. Configuration at NE (global) level.	Procedure 13-14

(1 of 3)

Feature ID	Feature or function	Description	See
Protocol enhancements			
SAM-13541	Template auto-creation of LDP targeted peers	The 5620 SAM supports the display of CLI template auto-created LDP targeted peers in the routing navigation tree. You can view properties but you cannot modify, shut down, or delete an auto-created LDP targeted peer that was created on an NE using a CLI template.	Procedure 23-16
SAM-22452	IS-IS—metric offsets for link group and link quality thresholds	You can create an IS-IS link group to bundle multiple member interfaces that are treated as a single virtual link for ECMP. You can create up to 8 bundles of IS-IS member interfaces. Each group behaves as single virtual link for ECMP purposes.	Procedures 23-21 and 23-23, 49-8
SAM-22625	RFE 150880—IS-IS instance level router ID configuration	You can configure the ISIS router ID value in each IS-IS instance, including the default instance. By default, the global value of router ID is used when an IS-IS instance is created. The IS-IS system ID for the instance continues to be derived from the router ID.	Section 23.1 Procedure 23-20
SAM-27516	RFE 150674—MVPN does not switch from *G to SG group with protocol protection enabled	You can enable the extraction and processing of PIM packets arriving at an NE inside a tunnel on a network interface in a protocol protection configuration.	*5620 SAM System Administrator Guide*
SAM-27520	RFE 155291	Configurable group interface source address for IGMP queries on base routing instance and VPRN site routing instance. Configurable query source IP address on IES site routing instance and VPRN group interface.	Procedures 23-46, 71-52, 70-6
Policy enhancements			
SAM-26072	PPTP ALG protocol option	The ALG Protocols parameter on a NAT policy supports the PPTP option.	Procedure 24-2
SAM-28843	RFE 160029	A WLAN-GW can insert the ISA RADIUS client IP address in NAS IP address attribute in authentication requests generated from ISA. Configurable NAS IP Address Origin in ISA RADIUS policy.	Procedure 49-8
SAM-30134	RFE 161438: SYSLOG: Support "-" as part of log-prefix	The 5620 SAM now supports including the "-" character in the body of the Message parameter string, provided that the character is not the first or last in the string.	Procedure 44-11
SAM-30529	RFE 160938: Match on AH/ESP NextHeader existence in IPv6 ACL line card filters	The 5620 SAM now supports matching on the presence or absence of IPv6 Authentication Headers and Encapsulating Security Payload Headers in ACL IPv6 filters.	Procedure 44-3
Service management enhancements			
SAM-22454	MPLS-TP Services—PW status signaling with status request support	A static PW status request message allows a peer that has a stale PW status for the far-end of a PW to request that the peer PE send a static PW status update. The 5620 SAM supports static PW status signaling with status request on: • Epipe VLL spoke SDP bindings • Cpipe VLL spoke SDP bindings • Apipe VLL spoke SDP bindings • VPLS spoke SDP bindings • IES spoke SDP bindings • VPRN spoke SDP bindings • mirror service spoke SDP bindings	Procedures 67-24, 68-45, 69-3, 69-4, 70-9, and 71-58

(2 of 3)

Feature ID	Feature or function	Description	See
SAM-22623	Show IOM/IMM label FIB information	You can use the Show FP Tunnel Table command on a routing instance to display the IOM/IMM label, next-hop, and outgoing interface information for BGP, LDP, and RSVP tunnels on the interface.	Procedure 22-31
SAM-27508	R-VPLS in BGP AD VPLS	You can configure BGP AD on routed VPLS, including routed I-VPLS and B-VPLS.	Chapter 68
SAM-27512	IANA VRF route type encoding compliance	You can configure a BGP site to change the type encoding of the VRF route import extended community used by NG-MPVN services to the IANA-compliant value using the IANA MVPN VRF Import Subtype parameter.	Procedure 23-2
SAM-27651	BGP Next Hop Unchanged	You can configure a BGP peer group to leave the BGP next hop unchanged when sending label-IPv4 routes to BGP peers using the Next Hop Unchanged parameter.	Procedure 23-4
SAM-28001	BGP IPv6 Multicast	The Family parameter on the VPN tab of BGP sites, groups, and peers supports the Multicast IPv6 option.	Chapter 23
SAM-28010	RFE 105360	You can configure IP MTU on IES and VPRN group interfaces.	Procedures 70-12 and 71-60
SAM-28845	RFE 159489—Improve service ID-based double hashing with ECMP and LAG	The hashing algorithm is improved on the ingress IOM when both ECMP and LAG are performed by the same NE. You can use the 5620 SAM to configure service ID LAG hashing to improve the LAG spraying of VLL service packets when both ECMP and LAG hashing are performed by the same NE.	Procedure 13-7
OAM and service testing enhancements			
SAM-12860	Improved timing accuracy for OAM delay measurements	Supported devices can now be configured to use the time recovered by PTP as the source of system time. This allows for improved accuracy in OAM delay measurements.	Procedure 15-10
SAM-22630	RFE 152308: ETH-CSF Reception Triggering Fault Propagation	Ethernet CSF frames are can now be processed by a MEG as an additional trigger for fault propagation on a receiving MEP.	Procedure 78-1
SAM-25105	Scale - Implement a mechanism of protection for retention setup	The DB test result retention time has been increased to a maximum of 720 hours. The 5620 SAM will automatically reduce the configured retention time based on the number of results and their incoming rate.	Refer to the *5620 SAM Parameter Guide*.
SAM-27658	RFE 155490: Support path-destination option with LDP-over-RSVP and LDP-BGP stitching	BGP label routes can now be specified for LSP or MPLS-TP LSP Ping and Trace OAM diagnostics.	Procedures 32-25 and 32-26
SAM-28019	RFE 151034: Implement hop-by-hop search for mtrace	The multicast trace test has been enhanced to ping neighboring NEs in a multicast group chain to determine which NE fails to respond.	Chapter 32

(3 of 3)

What's new in 5620 SAM Release 11.0 R6

5620 SAM Release 11.0 R6 is a maintenance release. No features have been added.

What's new in 5620 SAM Release 11.0 R5

Table 1-3 lists the features added in 5620 SAM Release 11.0 R5 and described in 5620 SAM core customer documentation.

Table 1-3 5620 SAM Release 11.0 R5 features

Feature ID	Feature or function	Description	See
GUI enhancements			
—	New filter type 'IS BLANK'	The 5620 SAM supports a new filter type, IS BLANK, for list window quick filters and advanced filtering.	Table 3-1
—	Export CSV files using UTF-8 with BOM encoding	The 5620 SAM supports exporting CSV files using UTF-8 with BOM encoding.	*5620 SAM System Administrator Guide*
SAM-336	Enhanced statistics plotting categorization	Each statistics class in the following drop-down lists has an icon that indicates the supported plot types: • Statistics Manager • Statistics tab of object properties form	"Graphing statistics overview" in the *5620 SAM Statistics Management Guide*
SAM-16574	Browse Examples of Scripts display enhancement	The Browse Examples of Scripts tree is optimized to present bundled scripts in bundles only.	"To browse and create from sample scripts, templates, and script bundles" in the *5620 SAM Scripts and Templates Developer Guide*
SAM-20246	Retain collapsible panels	The 5620 SAM supports saving the open or closed state of collapsible panels when a configuration form closes.	Section 3.1
SAM-21434	Enhanced selection of child objects in statistics plotter	When a Monitored Object in the Statistics Plotter window has one or more plottable child objects, the Monitored Object field is a drop-down selector for the child objects.	Procedure "To create a statistics graph" in the *5620 SAM Statistics Management Guide*
SAM-20315	Hide tabs on configuration forms	The 5620 SAM supports customization of tabs on a configuration form based on the user ID and object type. You can display, hide, or reorder tabs.	Procedure 3-20 Procedure 3-21
SAM-21571	Add workspaces to a user group	The 5620 SAM supports mandatory workspaces added to user groups.	*5620 SAM System Administrator Guide*
SAM-21545	Upgrades for saved workspaces from a previous release	The 5620 SAM supports adding new menu items to a saved workspace from a previous release.	Procedure 4-1
SAM-21995	Enhancements for Statistics UI Form	The Statistics tab of the properties form for some objects has separate child tabs for different groups of statistics counters.	"Tabular statistics view" in the *5620 SAM Statistics Management Guide*
SAM-22637	Regrouped tabs on service configuration forms	The tabs on service and site configuration forms have been regrouped to simplify navigation. The changes affect the following services and related sites: • VLL • VPLS • VPRN	Chapter 67 Chapter 68 Chapter 71
SAM-23981	Multi edit property forms	The 5620 SAM supports an enhanced multi-edit functionality on devices and property forms.	Chapter 3
Map enhancements			
SAM-788	Ethernet CFM on Composite Service Flat Map	This feature allows you to view and create CFM MEGs and tests from the Composite Service flat topology map.	Section 6.2 and 6.3 Procedures 6-27 and 6-32

(1 of 14)

Feature ID	Feature or function	Description	See
5620 SAM system management enhancements			
SAM-15196	KVM virtualization support	The 5620 SAM supports system deployment in a KVM virtual environment.	*5620 SAM Planning Guide*
SAM-15403	SSL certificate expiry management	When SSL is enabled in a 5620 SAM deployment, the 5620 SAM monitors the SSL certificate expiry and raises alarms when the expiry date is nearing and when the certificate is expired.	"Configuring SSL security" in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*
SAM-19983	Database tablespace consumption alarms	The 5620 SAM monitors the database tablespace capacity and raises alarms when the capacity is low.	—
SAM-22337	XML schema change summary table	The XML Schema Changes page includes a summary table with links to the change content.	*5620 SAM-O XML Reference*
Device management enhancements			
SAM-224	Subscriber data persistence	The 5620 SAM supports the configuration of NE file persistence for certain dynamic objects.	Procedure 13-22
SAM-15333	DCR 584557 - Remove GNE trap gap resynchronization	The 5620 SAM no longer supports trap resynchronization after the detection of a trap gap on a GNE.	—
SAM-19254	Management Suspended state for NEs	You can place a managed NE in a state of suspended management, which means that the 5620 SAM stops managing the NE, but retains the NE information.	Chapter 10
SAM-23815	OLC state for power supply trays	The 5620 SAM supports the configuration of the OLC state for power supply trays.	Procedure 15-20 *5620 SAM System Administrator Guide*
7210 SAS-D enhancements			
SAM-30648	Y.1564 test support on 7210 SAS-D and 7210 SAS-M (network)	5620 SAM support for Y.1564 bidirectional tests is extended to the 7210 SAS-D, Release 6.0 R2 or later.	Sections 77.9 and 77.10
7210 SAS-E enhancements			
7210 SAS-M enhancements			
SAM-22495	Support for bidirectional MIPs in Epipe services	The 5620 SAM Ethernet CFM function supports the creation of bidirectional MIPs for Epipe SAPs and SDPs configured on the 7210 SAS-M (in network mode), Release 6.0 R1 or later.	Procedure 78-1
SAM-30648	Y.1564 test support on 7210 SAS-D and 7210 SAS-M (network)	5620 SAM support for Y.1564 bidirectional tests is extended to the 7210 SAS-M (in network mode), Release 6.0 R2 or later.	Sections 77.9 and 77.10
7210 SAS-T enhancements			
SAM-20760	Support for the 7210 SAS-T device	The 5620 SAM supports management of the 7210 SAS-T and 7210 SAS-T ETR. Equipment and service support is similar to the 7210 SAS-M (in access-uplink mode), Release 6.0 R2. QoS support is similar to the 7210 SAS-D, Release 6.0 R2.	Section 8.5
7210 SAS-X enhancements			
SAM-31055	QoS override for access ingress queues	The 5620 SAM supports the configuration of policy overrides for access ingress policy queues applied to L2 access interfaces on the 7210 SAS-X, Release 6.0 R1 or later. Some restrictions apply.	Procedure 43-44

(2 of 14)

Feature ID	Feature or function	Description	See
SAM-22495	Support for bidirectional MIPs in Epipe services	The 5620 SAM Ethernet CFM function supports the creation of bidirectional MIPs for Epipe SAPs and SDPs configured on the 7210 SAS-X, Release 6.0 R1 or later.	Procedure 78-1
7450 ESS and 7750 SR enhancements			
SAM-12829	1588-2008 PTP support for 7750 SR-c12	The 5620 SAM supports the configuration of a 1588-2008 PTP clock on a 7750 SR-c12 equipped with a CFM XP B card.	Procedure 15-14 Procedure 15-15
SAM-13562	PTP time information	The 5620 SAM displays information about PTP time in the General tab of the PTP clock properties form. The following read-only parameters appear in the Time Properties Attributes panel: • Time Traceable • Frequency Traceable • PTP Timescale • PTP Time Source	—
SAM-19990	Automatic PAC FP3 IMM provisioning	When a supported PAC FP3 IMM is equipped in a card slot and provisioned, the daughter cards are automatically discovered and appear in the navigation tree.	Section 15.3
SAM-20251	NTP using IPv6	The 5620 SAM supports configuring IPv6 addresses for NTP associations, clients, peers or servers on the 7750 SR.	Procedure 15-10
SAM-23735	1588 ToD with hardware assistance	The 5620 SAM supports enabling 1588 PTP ToD hardware assistance on network interfaces and IES interfaces on the following MDAs: • 10-Port 1Gb XP SFP • 20-Port 1Gb XP SFPI • 1-Port 10Gb XP XFP • 2-Port 10Gb XP XFP • 4-Port 10Gb XP XFP • 4-Port 10Gb XP XFP IMM • 8-Port 10Gb XP XFP IMM The PTP HW Assist parameter can only be configured if the MDA has Sync-E enabled and the interface has a valid IPv4 address.	Procedure 22-10 Procedure 70-17
SAM-24165	LACP remote port information	The 5620 SAM displays information about the LACP partner of a LAG in the LACP tab of the LAG configuration form.	Section 14.10
SAM-25469	Configurable throttle rate for log events	The 5620 SAM supports throttle rate configuration for create and delete event traps on the 7750 SR, Release 11.0 R4 or later.	*5620 SAM System Administrator Guide*
SAM-25517	LLDP tunneling	The 5620 SAM supports enabling Dot1x tunneling on ports on the following nodes: • 7450 ESS • 7710 SR • 7750 SR • 7950 XRS The Tunneling parameter is located on the LLDP tab of the Port configuration form.	Procedure 16-1

(3 of 14)

Feature ID	Feature or function	Description	See
SAM-27490	Fine granularity BER thresholds	The 5620 SAM supports configuring fine granularity BER threshold parameters on 100G DWDM IMMs. The parameters appear in the Fine Granularity BER Thresholds panel of the Optical Transport Channel Unit tab on the port configuration form.	Procedure 16-1
SAM-27492	Rx-LOS threshold behavior for 100G DWDM interfaces	The 5620 SAM supports specifying the behavior of a 100G DWDM interface when the Rx-LOS threshold is reached, using the Rx LOS Reaction parameter on the Coherent Optics tab of the Port configuration form.	Procedure 16-1
SAM-28727	New IMM combination support	The 5620 SAM supports the configuration of a 2-PAC FP3 IMM card with the following combinations of daughter cards: • 1-port 100GE CFP and 10-port 10GE SFP	—
7705 SAR enhancements			
SAM-19794	OSPF on VPRN	The 5620 SAM supports the configuration of OSPF on a VPRN routing instance on the 7705 SAR, Release 6.0 R4 or later.	Procedure 71-50
SAM-19796	BGP Next-Hop-Self on route reflector	The 5620 SAM supports the configuration of a base router BGP instance to allow a route reflector of IP-VPN routes using its IP address as the next hop rather than BGP choosing the next hop, on Release 6.0 R4 or later.	Procedure 23-2
SAM-19813	Policy-based routing	The 5620 SAM supports the configuration of next hop routing on an ACL IP filter policy on the 7705 SAR, Release 6.0 R4 or later.	Procedure 44-2
SAM-19969	eBGP on base router	The 5620 SAM supports the configuration of eBGP on a base router on the 7705 SAR, Release 6.0 R4 or later.	Section 23.16
SAM-22012	T-LDP local LSR ID	The 5620 SAM supports the configuration of the local LSR ID on an LDP routing instance on the 7705 SAR, Release 6.0 R4 or later.	Procedure 23-16
SAM-22685	Adaptive clock recovery on MEF 8	The 5620 SAM supports the configuration of adaptive clock recovery on a 16/32 port DS1/E1 ASAP MDA and a i8/i16 port DS1/E1 ASAP MDA, Release 6.0 R4 or later.	Procedure 16-31
SAM-22689	Adaptive clock recovery on 7705 SAR-A	The 5620 SAM supports the configuration of adaptive clock recovery on a DS1/E1 ASAP MDA on the 7705 SAR-A, Release 6.0 R4 or later.	Procedure 16-31
SAM-28732	MWA backup and restore	The 5620 SAM supports the backup and restore of the radio database tar file for 7705 SAR NEs that have radios configured.	*5620 SAM System Administrator Guide*
7705 SAR-H enhancements			
SAM-22653	Firewall log policy	The 5620 SAM supports configuration of a firewall log policy on the 7705 SAR-H.	Procedure 60-5
SAM-24018	NTP support	The 5620 SAM supports configuring NTP on the 7705 SAR-H.	Procedure 15-10
SAM-28633	PoE Plus	The 5620 SAM supports PoE Plus with internal power supply on the 7705 SAR-H.	Procedure 16-19
7950 XRS enhancements			
SAM-12815	Support for soft reset on FP3-based line cards	The 5620 SAM supports performing a soft reset on XCM cards installed in a 7950 XRS, Release 11.0 R6 or later.	*5620 SAM System Administrator Guide*
SAM-14421	Routed VPLS support for 7950 XRS	The 5620 SAM supports the creation of Routed VPLS connectors for VPLS and I-VPLS sites on the 7950 XRS.	Procedure 68-7

(4 of 14)

Feature ID	Feature or function	Description	See
SAM-14437	Support for minor ISSUs	The 5620 SAM supports minor ISSUs for the 7950 XRS, Release 11.0 R6 and later.	*5620 SAM System Administrator Guide*
SAM-21238	Support of 6x40GE QSFP C-XMA	The 5620 SAM supports the 6x40GE QSFP C-XMA card for the 7950 XRS-20 and 7950 XRS-16c.	Section 8.16
SAM-21240	Support of 7950 XRS-16c	The 5620 SAM supports the discovery and management of the 7950 XRS-16c.	Section 8.16
SAM-23064	Apipe support for 7950 XRS	The 5620 SAM supports the creation of VLL Apipe services with sites on the 7950 XRS. The Apipe site must be a switching site, as Apipe SAPs are not supported on the 7950 XRS.	Procedure 67-8
OmniSwitch enhancements			
SAM-8852 SAM-15561	G.0832v2 support for AOS 6.4.5 R02 and AOS 7.3.1 NEs	The 5620 SAM supports the configuration of Ethernet Ring Elements using G.8032v2 on 6.4.5 R02 and 7.3.1 OmniSwitch NEs.	Procedure 27-7
SAM-14695	MC LAG support for AOS 6.4.5 NEs	The 5620 SAM supports the configuration of MC AOS groups on OS 6850E, OS 9700E, and OS 9800E, Release 6.4.5 or later.	Section 39.4
SAM-14697	ISSU support for stackable NEs	The 5620 SAM supports ISSU for OS 6400, OS 6850E, OS 6855, Release 6.4.5 R02 or later, in stacked configuration.	*5620 SAM System Administrator Guide*
SAM-22777	OS 6250 and OS 6450 AOS 6.6.4 support	The 5620 SAM supports the AOS Release 6.6.4 or later on the OS 6250 and OS 6450 switches.	Section 8.21
SAM-23456	Additional OS 6450 variations supported	The 5620 SAM supports new light models of the OS 6450.	Section 8.21
SAM-23458	Custom L2 profiles support	The 5620 SAM supports the creation of custom L2 profiles on the OS 6250M, Release 6.6.4 or later, and the OS 6450, Release 6.6.4 or later.	Procedure 52-3
SAM-25963	OS 6450-10 stacking support	The 5620 SAM supports stacking on the OS 6450-10, OS 6450-10L, OS 6450-P10, and OS 6450-P10L, Release 6.6.4 or later.	Procedure 15-30
SAM-25972	MEP ID used to target SAA test destination	The 5620 SAM supports use of the target's MEP ID in determining SAA test destination for CFM Loopback and CFM Two Way Delay tests. Applicable only to OmniSwitch NEs.	Procedure 32-7 Procedure 32-11
SAM-28988	Additional OS 10K card variation supported	The 5620 SAM supports the new OS10K-XNI-U32E card.	Section 8.21
Network management enhancements			
—	List ISA-WLAN GW groups and Soft GRE tunnels	The 5620 SAM lets you globally list ISA-WLAN GW groups and Soft GRE tunnels from the Manage→ ISA Functions→ ISA-WLAN main menu. ISA-WLAN GW groups can also be listed from Manage→ Equipment.	Section 14.8
SAM-742	DHCP failover support	Failover support on local DHCPv4 and DHCPv6 servers. Configurable on base routing instance and VPRN routing instance.	Section 65.4 Procedures 22-2, 22-3, and 22-4
SAM-13022	NAT and LNS reassembly	ISA-BB group reassembly configuration on base routing instance and VPRN site.	Procedures 22-1 and 71-3

(5 of 14)

Feature ID	Feature or function	Description	See
SAM-13028	Trap drop handling improvements	A windowing trap delayer option provides an enhanced method to resync the subscriber table in the event of a trap drop from an NE.	"To configure the windowing trap delayer option for subscriber table resyncs" in the *5620 SAM System Administrator Guide*
SAM-13062	RADIUS enhancements	• Session Timeout configuration on the PPP policy. • On the SLA profile, expanded range for the Category Timeout parameter. • On the RADIUS based accounting policy, expanded range for the Update Interval, Server Retry Attempts, and Server Timeout parameters. Support for three new RADIUS include attributes (Framed Route, Framed Ipv6 Route, and All Authorized Session Addresses). RADIUS server policy and Update Interval Jitter configuration. • On the Subscriber Authentication Policy, expanded range for the Retry Attempts and Timeout parameters. RADIUS server policy and Accounting Stop Message configuration. • On the local user database, PPP host, expanded range for the Password and Username parameters. RADIUS based accounting policy and duplicate RADIUS based accounting policy configuration. • On the local user database, DHCP host, RADIUS based accounting policy and duplicate RADIUS based accounting policy configuration. • On the RADIUS server policy, expanded range for the Timeout Seconds and Retry Attempts parameters. Support for Blocked State, Accounting Interim Minimum Interval, Accounting Interim Maximum Interval, Accounting Interim Lifetime, Accounting Stop Minimum Interval, Accounting Stop Maximum Interval, and Accounting Stop Lifetime configuration. • Accounting on/off configuration on the RADIUS server policy. • New accounting on/off group policy object. • On the RADIUS server policy, new Tools command to initiate Accounting On or Accounting Off messages from the NE.	Section 49.1 Procedures 54-4, 49-1, 49-4, 49-5, 49-6, and 65-5
SAM-13092	Dynamic block reservation	On a NAT pool configuration, dynamic port blocks can be reserved for the lifetime of a static port forward.	Section 24.1 and Procedure 24-3
SAM-13094	DS Lite/NAT64 fragmentation	IPv6 packet fragmentation support on DS Lite addresses and NAT64.	Section 24.1 and Procedure 24-3
SAM-13156	NAT traversal for IKEv2 remote access tunnel	You can enable NAT traversal support for IKEv2.	Procedure 29-1
SAM-15529	Minimum, maximum, and average value calculations in statistics plotter	The 5620 SAM Statistics Plotter legend now displays the minimum, maximum, and average values of the plot area defined by the slider position.	Procedure "To create a statistics graph" in the *5620 SAM Statistics Management Guide*
SAM-16581	Script methods to return object counts	Two Velocity script methods are available for counting network objects.	"Callouts" in the *5620 SAM Scripts and Templates Developer Guide*

(6 of 14)

Feature ID	Feature or function	Description	See
SAM-13543 SAM-9818	IP-IP tunneling support on the MS-ISA for the 7750 SR-7, 7750 SR-12, and 7750 SR-c12	An IP tunnel is a numbered IP interface of a private service, such as a VPRN or IES, that is associated with a private SAP to a tunnel group. You can configure IP tunnels, as well as GRE tunnels, on the tunnel interface under VPRN and IES services using the 5620 SAM.	Procedure 29-6
SAM-16886	Duplicate IP address alarms and search	The 5620 SAM raises an alarm if an IP address is used by more than one base router network interface or IES L3 interface in the network. You can search for duplicate IP addresses using the Network Resources tool.	Procedure 22-24
SAM-17958	Alarm history	The 5620 SAM allows you to search for historical alarms based on a specified time period.	Procedure 31-21
SAM-19232	DHCPv6 server attributes	Ignore Rapid Commit and Interface ID Mapping configuration on local DHCPv6 server. Prefix Type configuration on IPv6 address pool prefix.	Procedure 22-3
SAM-20241	Template execution using different scope of command profile	To ensure consistent service creation by multiple operators, you can specify a scope of command profile for service template execution that supersedes the operator scope of command profile.	"XML API template overview" in the *5620 SAM Scripts and Templates Developer Guide*
SAM-20798	RFE 123469 - MCS over hybrid ports	Enhancement to allow SRRP on hybrid ports, including hybrid ports in MCS with full ESM (including multicast). Supported on the 7750 SR Release 10.0 R10.	Procedure 40-1
SAM-21398	Script-based alarm generation	You can use a Velocity script method to generate a 5620 SAM alarm.	"Callouts" in the *5620 SAM Scripts and Templates Developer Guide*
SAM-21425	Plotting of normalized statistics for non-traffic statistics counters	You can plot rate-based statistics for non-traffic statistics counters, such as active subscriber hosts.	"Graphical statistics view" in the *5620 SAM Statistics Management Guide*
SAM-21429	Opening link endpoint plots from topology maps using plotter profiles	After you configure a plotter profile to include the other endpoint of a port-based link, you can use a right-click menu option on the link in a topology map to automatically begin plotting the endpoint data.	"Graphical statistics view" in the *5620 SAM Statistics Management Guide*
SAM-21495	Various scripting enhancements	The 5620 SAM supports the following script functions: • streaming XML File input • output to a file • script association with a specific object to enable right-click menu access to the script from the object	"Callouts" and "Script execution" in the *5620 SAM Scripts and Templates Developer Guide*
SAM-21517	NAT deterministic script	On NE properties, you can specify the URL of a remote server on which NAT deterministic script results are stored.	Section 24.1 and Procedure 24-4
SAM-21589	RFE 138556	In a NAT configuration, you can specify a standby routing instance in a redundant pool configuration for static port forward requests.	Section 24.1 and Procedure 24-3
SAM-21593	Enhanced multicast LAG hashing to enable per (S,G) hash over a LAG	You can configure an NE to send multicast traffic over a LAG.	Procedure 13-7
SAM-21715	Deterministic DS Lite	Configurable DS Lite maximum subscriber limit on deterministic NAT configuration.	Procedure 24-3

(7 of 14)

Feature ID	Feature or function	Description	See
SAM-21967	RFE 126552 - Subnet allocation based on system ID	Vendor specific option string configuration on IES and VPRN group interface, and subnet binding key configuration on local DHCPv4 server address pool. Allows local DHCP server to provide more subnets as the subscriber base grows, and remove them as the subscriber base shrinks.	Procedures 22-2, 70-12 and 71-60
SAM-22459	Additional Text Find icon	The 5620 SAM supports the Additional Text Find icon on the object property forms by enabling or disabling the Show Additional Text Button Properties Forms parameter on the Alarm Settings form.	Procedure 31-4
SAM-22749	Residential subscriber host mid-session change	You can configure the ANCP string and intermediate destination ID on a dynamic residential subscriber host. The Subscriber profile string, SLA profile string, and application profile string can be specified using a Select button, or typed as free text. All of the above parameters can be changed without re-instantiating the host.	Procedure 65-38
SAM-26040	Alarm Settings window	The 5620 SAM supports an enhanced form on the Alarm Settings window.	Chapter 31
SAM-26202	Residential subscriber instance information retrieved from network	The following read-only information on the Residential Subscriber Instance GUI form is read directly from the network (as opposed to being stored in the 5620 SAM database): • General tab - ANCP String, Intermediate Destination ID, Subscriber Profile, NAT Policy, Application Profile, Subscribed Application Profile, ISA-AA Group ID, Egress Secondary Shaper, RADIUS Egress Aggregate Rate Limit, Operational Egress Aggregate Rate Limit • ANCP Subscriber Line Rates tab - all information • Subscriber QoS Overrides tab - all information • Multicast CAC Status - all information	—
SAM-30508	RFE 161635	Maximum limit of active WLAN GW IOMs per WLAN GW group increased from four to five.	Section 14.8
—	Purging historical alarms	The 5620 SAM does not support manual purging of historical alarms from the Historical alarms form and the Alarm Settings form.	Chapter 31 *5620 SAM System Administrator Guide*
Protocol enhancements			
SAM-12960	MPLS-TP—OAM	Ping and trace tests are enhanced to support MPLS-TP LSPs.	Procedures 32-25 and 32-26
SAM-12962 SAM-19106 SAM-21305	MPLS-TP Services—PW status signalling without status request support	The 5620 SAM supports static PW status signaling on: • Epipe VLL spoke SDP bindings • Cpipe VLL spoke SDP bindings • Apipe VLL spoke SDP bindings • VPLS spoke SDP bindings • IES spoke SDP bindings • VPRN spoke SDP bindings • mirror service spoke SDP bindings Only static PW-to-static PW switching is supported.	Procedures 67-4, 67-5, 67-10, 67-11, 67-23, 67-24, 68-44, 68-45, 69-3, 69-4, 70-8, 70-9, 71-57, and 71-58

(8 of 14)

Feature ID	Feature or function	Description	See
SAM-12964 SAM-23494	MPLS-TP—LSR	MPLS-TP is a set of MPLS protocol functions that enables the use of MPLS in transport networks and applications. MPLS-TP provides in-band proactive OAM and protection mechanisms that do not rely on a control plane, such as RSVP-TE, to operate. MPLS-TP enables MPLS to be deployed in a statically configured transport network without the need for a dynamic control plane. The 5620 SAM provides simple provisioning for the network management support of MPLS-TP.	Chapter 26 Procedures 25-2 and 27-1
SAM-12968	Unnumbered interfaces on LDP	The 5620 SAM supports configuring an unnumbered interface as an LDP interface.	Procedure 23-14
SAM-12978	Automatic creation of RSVP-TE LSP mesh	The 5620 SAM supports two new LSP template types in addition to the existing P2MP LSP template for VPRN MVPN: • one-hop P2P • mesh P2P You cannot configure these template types using the 5620 SAM. When the templates are created using CLI, the 5620 SAM displays the templates as read-only. You cannot modify, distribute, or remove these template types using the 5620 SAM. When the templates are configured and associated with an auto-LSP using CLI, they automatically create dynamic LSPs. The 5620 SAM displays the dynamic LSPs. The dynamically created LSPs cannot be associated with SDPs. When you create VPRN MVPNs, the one-hop and mesh P2P template types are not listed when you select the MVPN Include Tunnel Template and the MVPN Selective Tunnel Template.	Procedure 25-24 Procedure 25-25
SAM-13014	IPv6 MVPN	The 5620 SAM supports all IPv6 multicast protocols in an MVPN instance. The IPv4 mLDP or RSVP-TE core carries IPv6 multicast traffic within IPv4 mLDP or RSVP-TE provider tunnels. The following is supported: • MLD on IES and VPRN routing instances • IPv6 PIM on VPRN routing instances and routing interfaces • IPv6 BFD for VPRN • BGP Family support for IPv6 MVPN	Procedures 23-2, 23-43, 23-59, 23-60, 23-61, 23-62, 71-38, 71-50
SAM-14196	MPLS auto-bandwidth based on forwarding class subset	The 5620 SAM supports sampling weight parameters for auto bandwidth forwarding classes on dynamic LSPs. These parameters allow you to change how the bandwidth rate is calculated by assigning different weight percentages to each forwarding class.	Section 25.1 Procedure 25-9
SAM-19104	BGP Deterministic MED	You can configure the BGP best path selection algorithm to group and compare all of the paths that belong to the same AS, when some of the paths originate from neighboring ASes or do not have a MED attribute.	Procedures 23-2 and 71-51
SAM-21764	IS-IS/OSPF LFA with multicast fast failover	An NE can select the active or standby paths using IS-IS and OSPF LFAs.	Procedure 23-40
SAM-23098	mVPN P2MP LSP navigation	You can navigate to a P2MP LSP from an mVPN inclusive tunnel.	Procedure 23-44

(9 of 14)

Feature ID	Feature or function	Description	See
SAM-24172	PE ID based MAC flush for interoperation with Cisco/Juniper	The 5620 SAM supports the configuration of an LDP peer to control the processing of the LDP PE-ID Tlv to handle the MAC flush for interoperation with Cisco and Juniper.	Procedure 23-15
Policy enhancements			
SAM-613	DCR 598650: Scheduling of policy audits	The 5620 SAM now allows policy audits to be added to the Scheduler functions.	Procedures 42-11, 7-1, and the *5620 SAM System Administrator Guide*.
SAM-667	Multiple distributions in one click	The 5620 SAM now allows multi-selection of most global policy types for distribution. The selected policies must all be of the same type.	Procedures 42-2 and 42-14
SAM-683	DCR 581270 - Audit mismatches with non-existent entry	This feature identifies differences between a policy entry that exists in both the global and a local versions of a policy. Conducting a policy audit indicates exactly which fields are different. This also includes missing entries.	Section 42.1 and Procedure 42-12
SAM-705	Distribution progress (OSSI part)	For OSS access, the 5620 SAM now sends a JMS message with the results of a policy distribution event. A task monitor is added to the distribution task.	The *5620 SAM XML OSS Interface Developer Guide*
SAM-706	DCR 509367 - Distribution supports NE groups	The 5620 SAM now supports policy distribution to groups of NEs. This is handled by creating a policy distribution group.	Section 42.1 and Procedures 42-1 and 42-3
SAM-11507	Queue Group Override at FP and Port levels for Access/Network Egress/Ingress	Support for queue group policer control overrides at the forwarding plane and port levels is added.	Procedure 15-26
SAM-12426	Improve creation of ACL filter entries	The 5620 SAM now supports copying ACL filter policy filter entries between policies.	Procedure 44-12
SAM-12802	Embedded ACL filters	The 5620 SAM introduces a new type of ACL filter policy. An embedded filter policy allows operators to define a common set of filter policy rules that can then be embedded in one or more ACL filter policies.	Section 44.1 and Procedure 44-13
SAM-12864	IPv4/IPv6 CPM filter port match enhancements (port range, port-list, port command)	The 5620 SAM now supports creating and specifying a Port List to use when matching source and destination TCP/UDP ports in CPM filter policies.	Procedure 44-6 and the *5620 SAM System Administrator Guide*
SAM-13749	DCR 627591: Switch distribution mode on CLI change	The 5620 SAM now enables a policy change made using CLI to switch the distribution mode for certain types of local policies to Local Edit Only.	Procedure 42-1, and the *5620 SAM System Administrator Guide*. Also refer to the "Switch Distribution Mode to Local Edit Only on CLI Change" parameter in the *5620 SAM Parameter Guide*.
SAM-15081	Auto-generation of filter prefix lists (IOM filter support)	The 5620 SAM now supports the auto-generation of IP Prefix Lists for both IPv4 and IPv6 ACL IP filter policies.	Procedures 44-5, 44-2, and 44-3
SAM-20430	Policy exclusive edit command	The 5620 SAM now supports setting a "Use Exclusive Edit" parameter for an NE to prevent its local policy definitions from being changed by global updates.	Procedure 13-9

(10 of 14)

Feature ID	Feature or function	Description	See
SAM-21735	Shared filter terms from RADIUS	High watermark and low watermark alarm threshold configuration for dynamically-inserted filter count on ACL IP filter policy and ACL IPv6 filter policy.	Section 44.1 Procedures 44-2 and 44-3
SAM-21971	RFE 141452 - QoS on mobile gateway profile	Support for PGW and GGSN QoS configuration on mobile gateway profile.	Procedure 54-13
SAM-21973	RFE 141457 - charging characteristics on mobile gateway profile	Support for charging characteristic configuration on mobile gateway profile.	Procedure 54-13
SAM-23177	DCR 658552: Add description to prefix list member	A Description field was added to the prefix list policy to allow entering descriptive text.	Procedure 22-16
SAM-23199	DCR 658548: New tabs needed for Routing Policy, Prefix list and Community	The 5620 SAM now allows you to display a list of NEs currently using global or local versions of certain routing policy types.	Procedure 22-26
SAM-24945	Add Filter Log and SysLog Policy	The 5620 SAM now allows you to configure a Filter Log and Sys Log for use with IP, IPv6, and MAC filter entries.	Procedures 44-10 and 44-11
SAM-25600	Ageout constraint policy	The ageout constraint policy defines a configurable ageout interval for a specified object type, after which objects are deleted from the 5620 SAM database.	Chapter 56 Procedure 56-2
SAM-27553	Aggregation Scheduler visibility at Port and Card levels	The 5620 SAM now lists associated aggregation schedulers in the Aggregation tab of the properties form of an assigned card or port (including LAGs).	Procedure 43-31
SAM-30695	Policy Synchronization Improvement	Changes were made to the policy synchronization GUI: • Distribution Mode button was renamed to Switch Distribution Mode • Available and destination instances panels were renamed	Procedures 42-1 and 42-7, and the *5620 SAM System Administrator Guide*.
Service management enhancements			
SAM-736	Managed routes	The 5620 SAM can retrieve managed route information from the NE for hosts instantiated on IES and VPRN services.	Section 65.4
SAM-12877	SAP and SDP binding loopback with MAC swap	The 5620 SAM supports the creation of a service throughput configuration that uses a SAP or MPLS SDP binding with loopback enabled as the traffic test destination. SAP and SDP binding loopbacks are supported for sites in Epipe and VPLS services on the 7450 ESS, 7750 SR, and 7950 XRS Release 11.0R4.	Procedure 81-1
	Service throughput configuration enhancements	The following enhancements have been made to service throughput configurations: • You can configure multiple service throughput tests on a service. • Existing service throughput configurations are listed on the Throughput Configuration tab of a service or composite service.	Chapter 81
SAM-12915	Configurable OSPF redistribution timers	You can configure the redistribution timers on an OSPF site to adjust the delay before a different external route is sent using OSPF.	Procedure 23-30

(11 of 14)

Feature ID	Feature or function	Description	See
SAM-12992	BGP VPWS support	The 5620 SAM supports the configuration of a BGP VPWS. A BGP VPWS is an L2 VPN that uses BGP signaling to establish pseudowires. BGP VPWS is supported on the 7450 ESS, 7710 SR, 7750 SR, and 7950 XRS, Release 11.0R1.	Section 67.1 Procedure 67-54
SAM-13006	PW SAP for IES and VPRN services	You can choose a PW port as the terminating port for an L3 access interface on an IES or VPRN service. The PW port must be bound to a service tunnel.	Procedure 70-17 Procedure 71-22
	Secondary shaper support for PW port binding	You can specify an HSMDA egress secondary shaper for a PW port binding using the PW SAP Secondary Shaper parameter. The parameter only appears when you configure a PW port binding for an HSMDA port.	Procedure 27-1
SAM-13012	PIM, OSPF, IGMP, MVPN support on carrier carrier VPN VPRNs	You can configure PIM, OSPF, IGMP, and MVPN on a VPRN service that has the Carrier Carrier VPN parameter enabled.	Chapter 71
SAM-13024	Vport-aware H-QoS adjustment for multicast	Egress Rate Modify status configuration on virtual ports for ATM or Ethernet ports.	Procedures 63-1 and 63-2
SAM-13046	DHCP server multihoming enhancements	Address assignment configuration on IES and VPRN group interfaces. DHCP server synchronization configuration on IES and VPRN subscriber interfaces.	Procedures 70-10, 70-12, 71-59, and 71-60
SAM-13122	AA ICAP URL filtering	You can apply parental-control filtering to AA traffic.	Chapter 76
SAM-16140	RPF Vector support	The 5620 SAM supports configuring RPF vector processing on a PIM site for use with an option-C or option-B draft-Rosen Inter-AS MVPN. The RPF Vector parameter must be configured on each site in the MVPN.	Procedure 23-40
SAM-17706	Service Type field in Service Manager	The Service Type column is added to the Manage Services form for all 5620 SAM services.	—
SAM-19662	Support for application filter protected ranges	When you renumber a range of AA application filters, you can specify an end value to exercise greater control over the allocation of filter IDs.	Chapter 76
SAM-19889	Static B-MACs and ISIDs for connection to non-SPB-managed networks	You can configure static B-MACs and static ISIDs to allow an SPB interface to be configured on a SAP or spoke SDP binding that is not part of the SPB network or region. This allows SPB networks to interface to other PBB networks that use other control planes. Static B-MACs allow remote PBB Epipes to connect to SPB managed networks. Static ISIDs allow I-VPLS services to connect to non-SPB I-VPLS services. You can create an ISID policy to specify the use of the default multicast tree and suppression of the advertisement of ISIDs in SPB when I-VPLS or static ISIDs are used for unicast services. Static B-MACs and static ISIDs are supported on SAPs and spoke SDP bindings, and SAPs on MC-LAGs.	"SPB in VPLS" in section 68.1 Procedures 68-67, 68-68, and 68-69
SAM-19895	PPPoE remote ID and circuit ID on LUDB	Remote ID and circuit ID configuration on PPP hosts on local user database.	Procedure 65-5
SAM-20846	DHCPv6 Route Populate on VPRN and IES	The 5620 SAM supports configuring route populate parameters on L3 access interfaces in VPRN and IES services, and specifying DHCPv6 protocols as part of the From Criteria in a policy statement entry.	Procedure 70-44 Procedure 71-47 Procedure 22-15

(12 of 14)

Feature ID	Feature or function	Description	See

SAM-21870	Service and composite service states	The overall service and composite service states are simplified to include only the following operational flags to determine the Aggregated Operational Status of a service or composite service:
		• Services
		  • Site(s) Down
		  • SDP Binding(s) Down
		  • Monitored Access(es) Down
		• Service sites
		  • SDP Binding(s) Down
		  • Monitored Access(es) Down
		• Composite services
		  • Service Component Degraded
		The Composite Service Aggregated Operational State depends on the aggregated operational state or states of the services that are associated with it.
			—

SAM-21951	BFD on LAG support	The 5620 SAM supports the configuration of BFD on an ethernet LAG. When you enable BFD on a LAG, the 5620 SAM creates micro-BFD sessions for each link in the LAG.	Section 14.10 Procedure 14-15 Procedure 14-16
SAM-21963	BGP split horizon support	The 5620 SAM supports the configuration of Split Horizon parameter on BGP sites and peer groups on base routers and in VPRN services.	Procedure 23-2 Procedure 23-4 Procedure 71-51
SAM-22137	OSPFv3 as PE-CE protocol in VPRNs	You can create multiple OSPFv3 instances on a VPRN, and add L3 access to those instances.	Section 71.1 Procedure 71-6
SAM-22160	AA application import script	When a new set of AA applications is available from Alcatel-Lucent, you can import the application set using the 5620 SAM script management function.	Chapter 76
SAM-22232	Re-evaluate lease states	The 5620 SAM Re-evaluate Lease States function allows SLA profile or subscriber profile changes on residential subscribers without re-instantiating the hosts.	See chapter 65 and Procedure 65-33.
SAM-22613	Cflowd for L2 interfaces on VPLS and EPipe services	The 5620 SAM supports enabling ingress Cflowd for L2 access interfaces on sites and i-sites in VPLS, MVPLS, and Epipe services.	Procedure 67-27 Procedure 68-24
SAM-22747	AA HTTP enrichment	You can configure an AA HTTP enrichment policy for a 7750 SR and use it as the action criterion in an application QoS entry.	Chapter 76
SAM-24151	List dynamically created objects on an NE	The 5620 SAM supports displaying lists of dynamically created objects on an NE, including sites and SAPs. The list of dynamic SAPs is automatically updated; lists of other objects must be retrieved from the NE.	Procedure 75-3
SAM-24159	HTTP content insertion for in-browser notification	You can configure an HTTP notification policy and associate it with an AQP on an AA group or partition.	Chapter 76
SAM-24163	Upstream Multicast Hop to mVPN	You can configure the Unicast Route Preference option for the US Multicast Hop Selection under mVPN for VPRN PIM sites.	Procedure 23-41
SAM-24177	RFE 147085	Support for RADIUS-communicated pools for SLAAC IP address assignment. IPv6 address assignment configuration on IES and VPRN group interfaces.	Procedures 70-12 and 71-60
SAM-24179	RFE 147082	WLAN Gateway IPv6 Address configuration on IES soft GRE group interface.	Procedure 70-13

(13 of 14)

Feature ID	Feature or function	Description	See
SAM-24478	G8032 Ethernet ring discovery	The 5620 SAM automatically discovers G8032 Ethernet rings and creates the related paths and interconnects. You can also perform an Ethernet ring audit to discover new rings, or troubleshoot problems with existing rings.	Chapter 27 Procedure 27-16
SAM-24558	DTS 104244 - DHCP unique identifier	Server ID configuration for local DHCPv6 server on routing instance, VPRN routing instance, VPRN group interface, and IES group interface.	Procedures 22-3, 70-12, and 71-60
OAM and service testing enhancements			
SAM-777	Re-generation of MEG/MEP/Tests upon service topology change	This feature allows objects (SDP bindings, SAPs, and applicable CFM tests) in the MEG and MEG sub-groups to automatically change in response to topology changes in a service or composite service.	Procedure 78-1
SAM-788	Ethernet CFM on Composite Service Flat Map	This feature allows you to view and create CFM MEGs and tests from the Composite Service flat topology map.	Section 6.2 and 6.3 Procedures 6-27 and 6-32
SAM-792	One-time Service/Composite Service test validation	The 5620 SAM supports running a one-time test validation. This permits quickly testing a service or composite service, either during provisioning or after activation. A variety of services and transport components can be tested.	Procedures 77-9, 25-12, 27-15, 66-10, 67-46, 68-73, 71-67, and 74-7
SAM-933	Auto creation of MEG, MEPs (and MIPs) for G8032 ring segs	The 5620 SAM provides a mechanism to automatically generate OAM objects for ethernet rings. Global MEGS, MEPs, and MIPs are included.	Procedure 27-8
SAM-12882	802.3ah enhancements - ISSU operation	The 5620 SAM now supports a "Grace Tx State Enable" parameter which allows an NE to locally execute a grace period. When the grace period is enabled, all peer timeouts are extended locally and an eligible EFM-OAM entity transmits grace period information.	Procedure 32-42
SAM-15436	DCR 594961: Display Service Test Status on managed services	The 5620 SAM now displays a Test Suite Count indicator to show the number of configured test suites that a specific test entity is currently associated with.	Procedures 77-4
Additional features			
5620 SAM documentation enhancements			
—	Creation of a new *5620 SAM MPR User Guide*	Consolidates the tasks performed by a user to discover, configure, and manage 9500 MPR and 9500 MPRe devices using the 5620 SAM. This guide is intended to be used in conjunction with the *5620 SAM User Guide*.	*5620 SAM MPR User Guide*

(14 of 14)

What's new in 5620 SAM Release 11.0 R4

5620 SAM Release 11.0 R4 is a maintenance release. No features have been added.

What's new in 5620 SAM Release 11.0 R3

Table 1-4 lists the features added in 5620 SAM Release 11.0 R3 and described in 5620 SAM core customer documentation.

Table 1-4 5620 SAM Release 11.0 R3 features

Feature ID	Feature or function	Description	See
7210 SAS-D enhancements			
SAM-14715	Transit service enhancements	The 5620 SAM extends support for transit services for the 7210 SAS-D, Release 4.0 R7 or later, to include: • alarm association • listing of transit services • listing of transported services	Section 27.3
SAM-22480	Support of 7210 SAS Release 6.0 R1 in SAM 11.0R3	The 5620 SAM supports Release 6.0 R1 for the 7210 SAS-D.	—
SAM-22482	QoS override	The 5620 SAM supports policy overrides for access ingress policy meters applied to L2 access interfaces on the 7210 SAS-D, Release 6.0 R1 or later. Some restrictions apply.	Procedure 43-43
SAM-22487	DHCP relay support for 7210 SAS	The 5620 SAM supports configuring DHCP relay on the 7210 SAS, Release 6.0 R1 or later.	Procedure 68-34
SAM-22491	IPv6 SSH	The 5620 SAM supports SSH access for CLI sessions on 7210 SAS NEs with IPv6 management addresses. This feature is supported on the 7210 SAS-D, Release 6.0 R1 or later.	Sections 9.2, 10.1, and 10.4 Procedures 10-2, 10-6, and 11-2
SAM-22493	Support for two WRED slopes	The 7210 SAS supports three WRED slopes per queue: • high priority TCP • low priority TCP • non-TCP With this feature, you can specify that only the high and low priority TCP slopes are used, and non-TCP slopes are ignored. The 5620 SAM supports two WRED slopes for the 7210 SAS-D, Release 6.0 R1 or later.	Procedure 13-18
SAM-27638	Dot1x tunneling on uplink	The 5620 SAM supports 802.1x authentication tunneling for the 7210 SAS-D, Release 6.0 R1 or later.	Procedure 16-1
SAM-27817	Reboot Upgrade support for 7210 SAS	The 5620 SAM supports performing the Reboot Upgrade action on 7210 SAS nodes. However, you cannot use an upgrade policy to trigger a Reboot Upgrade on a 7210 SAS node.	*5620 SAM System Administrator Guide*
7210 SAS-E enhancements			
SAM-21561	1830 VWM flexible CWDM clip-on module support	The 1830 VWM is an add-on optical module that attaches to the USB port of a 7210 SAS device. The 5620 SAM supports the configuration of an equipment shelf for the 1830 VWM on the 7210 SAS-E, Release 5.0 R4 or later.	Procedure 15-2
SAM-22480	Support of 7210 SAS Release 6.0 R1 in SAM 11.0R3	The 5620 SAM supports Release 6.0 R1 for the 7210 SAS-E.	—
SAM-22482	QoS override	The 5620 SAM supports policy overrides for access ingress policy meters applied to L2 access interfaces on the 7210 SAS-E, Release 6.0 R1 or later. Some restrictions apply.	Procedure 43-43
SAM-22487	DHCP relay support for 7210 SAS	The 5620 SAM supports configuring DHCP relay on the 7210 SAS, Release 6.0 R1 or later.	Procedure 68-34

(1 of 5)

Feature ID	Feature or function	Description	See
SAM-22491	IPv6 SSH	The 5620 SAM supports SSH access for CLI sessions on 7210 SAS NEs with IPv6 management addresses. This feature is supported on the 7210 SAS-E, Release 6.0 R1 or later.	Sections 9.2, 10.1, and 10.4 Procedures 10-2, 10-6, and 11-2
SAM-27817	Reboot Upgrade support for 7210 SAS	The 5620 SAM supports performing the Reboot Upgrade action on 7210 SAS nodes. However, you cannot use an upgrade policy to trigger a Reboot Upgrade on a 7210 SAS node.	*5620 SAM System Administrator Guide*
7210 SAS-M enhancements			
SAM-14705	ITU-T Y.1564 test-head support for 7210 SAS-M Nodes	The 5620 SAM supports test-head functionality and Y.1564 bidirectional tests for service configuration and throughput on the 7210 SAS-M, Release 5.0 R4 or later.	Sections 77.9 and 77.10
SAM-14715	Transit service enhancements	The 5620 SAM extends support for transit services for the 7210 SAS-M (in access-uplink mode), Release 4.0 R7 or later, to include: • alarm association • listing of transit services • listing of transported services	Section 27.3
SAM-21561	1830 VWM flexible CWDM clip-on module support	The 1830 VWM is an add-on optical module that attaches to the USB port of a 7210 SAS device. The 5620 SAM supports the configuration of an equipment shelf for the 1830 VWM on the 7210 SAS-M, Release 5.0 R4 or later.	Procedure 15-2
SAM-22436	Hybrid ports support	The 5620 SAM supports hybrid mode when you configure Ethernet ports on the 7210 SAS-M (Network mode), Release 6.0 R1 or later.	Procedures 16-1, 16-15
SAM-22480	Support of 7210 SAS Release 6.0 R1 in SAM 11.0R3	The 5620 SAM supports Release 6.0 R1 for the 7210 SAS-M.	—
SAM-22482	QoS override	The 5620 SAM supports policy overrides for access ingress policy meters applied to L2 access interfaces on the 7210 SAS-M, Release 6.0 R1 or later. Some restrictions apply.	Procedure 43-43
SAM-22487	DHCP relay support for 7210 SAS	The 5620 SAM supports configuring DHCP relay on the 7210 SAS, Release 6.0 R1 or later.	Procedure 68-34
SAM-22489	SRLG policy support for 7210 SAS	The 5620 SAM supports distributing SRLG policies to the 7210 SAS-M and 7210 SAS-X, Release 6.0 R1 or later.	Procedures 22-22 and 22-23
SAM-22491	IPv6 SSH	The 5620 SAM supports SSH access for CLI sessions on 7210 SAS NEs with IPv6 management addresses. This feature is supported on the 7210 SAS-M, Release 6.0 R1 or later.	Sections 9.2, 10.1, and 10.4 Procedures 10-2, 10-6, and 11-2
SAM-22493	Support for two WRED slopes	The 7210 SAS supports three WRED slopes per queue: • high priority TCP • low priority TCP • non-TCP With this feature, you can specify that only the high and low priority TCP slopes are used, and non-TCP slopes are ignored. The 5620 SAM supports two WRED slopes for the 7210 SAS-M, Release 6.0 R1 or later.	Procedure 13-18

(2 of 5)

Feature ID	Feature or function	Description	See
SAM-22497	OSPF IP ECMP	The 5620 SAM supports ECMP routing for the 7210 SAS-M (in network mode), Release 6.0 R1. The device system resource profile must be appropriately configured.	Procedures 13-20 and 22-1
SAM-27638	Dot1x tunneling on uplink	The 5620 SAM supports 802.1x authentication tunneling for the 7210 SAS-M (in access-uplink mode), Release 6.0 R1 or later.	Procedure 16-1
SAM-27817	Reboot Upgrade support for 7210 SAS	The 5620 SAM supports performing the Reboot Upgrade action on 7210 SAS nodes. However, you cannot use an upgrade policy to trigger a Reboot Upgrade on a 7210 SAS node.	*5620 SAM System Administrator Guide*
7210 SAS-X enhancements			
SAM-1245	Hierarchical ingress QoS (ingress queuing)	The 5620 SAM supports the configuration of HQoS queues for 7210 SAS access ingress policies. When deployed, the HQoS policies can be attached to L2 access interfaces on the 7210 SAS-X, Release 5.0 R4 or later. You can allocate resources for this function in the system resource profile. Aggregate rate shaping is also supported when you attach the policy to a SAP.	Sections 8.5 and 43.1 Procedures 13-20, 43-2, 67-28, 68-25, and 70-22
SAM-21561	1830 VWM flexible CWDM clip-on module support	The 1830 VWM is an add-on optical module that attaches to the USB port of a 7210 SAS device.The 5620 SAM supports the configuration of an equipment shelf for the 1830 VWM on the 7210 SAS-X, Release 5.0 R4 or later.	Procedure 15-2
SAM-22436	Hybrid ports support	The 5620 SAM supports hybrid mode when you configure Ethernet ports on the 7210 SAS-X, Release 6.0 R1 or later.	Procedures 16-1, 16-15
SAM-22480	Support of 7210 SAS Release 6.0 R1 in SAM 11.0R3	The 5620 SAM supports Release 6.0 R1 for the 7210 SAS-X.	—
SAM-22482	QoS override	The 5620 SAM supports policy overrides for access ingress policy meters applied to L2 access interfaces on the 7210 SAS-X, Release 6.0 R1 or later. Some restrictions apply.	Procedure 43-43
SAM-22487	DHCP relay support for 7210 SAS	The 5620 SAM supports configuring DHCP relay on the 7210 SAS, Release 6.0 R1 or later.	Procedure 68-34
SAM-22489	SRLG policy support for 7210 SAS	The 5620 SAM supports distributing SRLG policies to the 7210 SAS-M and 7210 SAS-X, Release 6.0 R1 or later.	Procedures 22-22 and 22-23
SAM-22491	IPv6 SSH	The 5620 SAM supports SSH access for CLI sessions on 7210 SAS NEs with IPv6 management addresses. This feature is supported on the 7210 SAS-X, Release 6.0 R1 or later.	Sections 9.2, 10.1, and 10.4 Procedures 10-2, 10-6, and 11-2
SAM-22497	OSPF IP ECMP	The 5620 SAM supports ECMP routing for the 7210 SAS-X, Release 6.0 R1. The device system resource profile must be appropriately configured.	Procedures 13-20 and 22-1
SAM-27817	Reboot Upgrade support for 7210 SAS	The 5620 SAM supports performing the Reboot Upgrade action on 7210 SAS nodes. However, you cannot use an upgrade policy to trigger a Reboot Upgrade on a 7210 SAS node.	*5620 SAM System Administrator Guide*
7705 SAR enhancements			

(3 of 5)

Feature ID	Feature or function	Description	See
SAM-11313	1+1 HSB protection support	The 5620 SAM supports the configuration, discovery, and operational state of an integrated MPT radio on the 7705 SAR-8 and 7705 SAR-18. The protection state is displayed on the links and 1+1 links are grouped in a common link group.	Sections 6.2 and 8.9 Procedures 15-11 and 15-12
SAM-16226	MEF 8 support on 2p channelized OC3 and 4p DS3	The 5620 SAM supports MEF 8 on the 2-port channelized OC3 and 4-port DS3 cards on the 7705 SAR-8 and 7705 SAR-18, Release 6.0 R2 or later. MEF 8 allows TDM services to be emulated across Epipe services using circuit emulation.	Section 67.1 Procedure 67-27
SAM-19798	SDI port Hold Time Up and Hold Time Down	The 5620 SAM supports Hold Time Up (milliseconds) and Hold Time Down (milliseconds) on RS-232 ports on SDI cards.	Procedure 16-32
SAM-20711	TWAMP server support	The 5620 SAM supports the configuration of a TWAMP server on the 7705 SAR, Release 5.0 R1 or later.	Section 8.9 Procedure 13-11
SAM-21180	Scheduled statistics support for SNMP based counters	The 5620 SAM supports scheduling of performance statistics for the 7705 SAR MIBs.	*5620 SAM Statistics Management Guide*
SAM-22010	ACL VLAN filter policy support on 2 port ring MDA	The 5620 SAM supports the configuration of an ACL VLAN filter policy on a 2-port ring MDA on the 7705 SAR, Release 6.0 R1 or later.	Procedures 16-1 and 44-4
SAM-22014	SSM on 2p 10G ring MDA	The 5620 SAM supports SSM on a 7705 SAR 2-port 10 Gig ring MDA.	Section 8.9
SAM-22659	MAC pinning on 2p 10G ring MDA	The 5620 SAM supports MAC pinning on a 7705 SAR 2-port 10 Gig ring MDA.	Procedure 15-33
SAM-22660	CFM Loopback on ring ports on 2P 10Gig Ring card	The 5620 SAM supports the configuration of CFM loopback on the ring port of a 2-port 10 Gig ring card on the 7705 SAR, Release 6.0 R3 or later.	Procedure 16-1
SAM-22662	Differential clock on 7705 SAR-A MDA	The 5620 SAM supports differential clock recovery on a 7705 SAR-A MDA, Release 6.0 R2 or later.	Procedures 15-33, 16-31, and 16-34
SAM-22664	IEEE 1588 edge time stamps on 7705 SAR-A and 7705 SAR-W	The 5620 SAM supports the collection of statistics for IEEE 1588 PTP timestamps on the 7705 SAR-A and 7705 SAR-W. The 5620 SAM supports the configuration of the Time of Day message type and output on the 7705 SAR-A.	Chapter 15, Procedure 16-1 *5620 SAM Statistics Management Guide* Procedure 13-2
SAM-22668	Pseudo-wire status signaling on the VPLS service	The 5620 SAM supports pseudo-wire status signaling on the VPLS service.	Procedure 68-44
SAM-22670	Pseudo-wire status signaling on the VLL Epipe service	The 5620 SAM supports pseudo-wire status signaling on the VLL Epipe service.	Procedure 67-4
SAM-22672	Differential clock recovery on 4p channelized DS3 cards and ports	The 5620 SAM supports differential clock recovery on a 4-port channelized DS3 card and DS3 port with CEM encapsulation on the 7705 SAR, Release 6.0 R3 or later.	Procedures 15-33, 16-31, and 16-34
SAM-22678	2 port ring MDA WAN support	The 5620 SAM supports WAN mode on a 2-port 10 Gig ring MDA Ethernet port on the 7705 SAR, Release 6.0 R2 or later.	Section 8.9 Procedure 16-1
SAM-23055	Auxiliary alarm definition on an Ethernet port	The 5620 SAM supports the configuration of an auxiliary alarm definition with trigger input on an Ethernet port on the 7705 SAR, Release 6.0 R1 or later.	Procedure 15-13

(4 of 5)

Feature ID	Feature or function	Description	See
SAM-24661	DHCP loopback	The 5620 SAM supports the configuration of DHCP loopback on a VPRN service L3 access interface on the 7705 SAR, Release 5.0 R1 or later.	Procedure 71-22
SAM-25483	Multicast address support for MEF 8 remote mac	The 5620 SAM supports multicast address for MEF 8 remote MAC on the 7705 SAR.	Section 67.1 Procedure 67-39
SAM-27930	Scheduler mode on SAP ingress and egress	The 5620 SAM supports the configuration of 4-Priority or 16-Priority scheduler modes for egress and ingress Ethernet interface aggregation schedulers on the 7705 SAR, Release 6.0 R1 or later.	Procedures 16-1, 67-29, 68-26, 70-23, and 71-26
9500 MPR/9500 MPRe enhancements			
SAM-5982	NTP configuration for date and time	The 5620 SAM supports the configuration of NTP for date and time on the 9500 MPR.	Procedure 15-10
SAM-12666	NEtO distribution - 4.2 Multi-version	The 5620 SAM supports NEtO distribution of the 4.2 Multi-version on the 9500 MPR and 9500 MPRe, in addition to 4.1, 4.0, and 3.4 releases.	–
SAM-21786 SAM-21788	1+1 MPT -xC over core card support	The 5620 SAM supports MPT-HC/MC pair protection configuration on the 9500 MPR core-enhanced card.	Chapter 8
SAM-21790	MPT-HL connected to Core-E/MSS-1 SFP port	The 5620 SAM supports an MPT-HL connection to the Core-E/MSS-1 SFP port in a 1+0 radio configuration.	Chapter 8
SAM-21792	SNMP support of PPP table for adjacent node auto discovery over radio port (9500 MPRe)	The 5620 SAM supports SNMP for adjacent node auto discovery over a 9500 MPRe radio port.	–
SAM-21798	Enhanced fan tray	The 5620 SAM supports the configuration of an enhanced fan tray with relay alarm points on the 9500 MPR, Release 4.2 or later.	–
SAM-21800	SNMP for G.826 radio PM	The 5620 SAM supports SNMP for G.826 radio PM (current and historical data) on the 9500 MPRe.	–
SAM-21861	VLAN topology view observation with P2MP extension	During the creation of VLAN services, intermediate sites are automatically added to the service topology view.	Procedure 66-1
SAM-21862	VLAN service with radio port as endpoint	The 5620 SAM supports a radio port as an access interface on a hop-based VLAN service on the 9500 MPR.	–
SAM-21903	ERPS ring services discovery button	The 5620 SAM supports a button for discovery of ERPS ring services on the 9500 MPR.	–

(5 of 5)

What's new in 5620 SAM Release 11.0 R2

5620 SAM Release 11.0 R2 is a maintenance release. No features have been added.

What's new in 5620 SAM Release 11.0 R1

Table 1-5 lists the features added in 5620 SAM Release 11.0 R1 and described in 5620 SAM core customer documentation.

Table 1-5 5620 SAM Release 11.0 R1 features

Feature ID	Feature or function	Description	See
GUI enhancements			
—	Copy Property Form Identifier	The 5620 SAM supports the Copy Property Form Identifier function. This is applicable to property, alarms and statistic forms.	Procedure 3-16
SAM-340	Workspace customization	The 5620 SAM supports the customization of menus, toolbars, tree labels, topology icon labels and window layout selections on the 5620 SAM GUI.	Procedures 4-1, 4-2, 4-3, 4-4, and 4-5
		You can export and import workspaces using the 5620 SAM GUI.	Procedures 4-9 and 4-10
		You can add or delete workspaces in the Workspaces tab of the User Preferences form. You can select workspaces from the workspace selector combo box on the 5620 SAM GUI.	Procedure 4-8
		The 5620 SAM supports the following scope of command roles for workspace management, import and export and public control: • administrator • user management • SAM management and operations	*5620 SAM System Administrator Guide*
SAM-12825	LAG egress QoS optimization	You can reduce the number of egress resources consumed by each SAP on a LAG by enabling the Per Forwarding Path Egress Queue parameter.	Procedures 14-10 and 14-11
SAM-13652	Go To Property Form	The 5620 SAM supports the enhancement of the Go To Property form function. A user can copy window identifiers and paste the information into trouble tickets or send them to peers.	Procedure 3-17
SAM-13431	Custom properties on NE configuration forms	The 5620 SAM supports custom properties that are configured using the System Preferences form; for example, location and site name. The custom properties can also be configured using the 5620 SAM-O.	*5620 SAM System Administrator Guide* *5620 SAM-O XML Reference*
SAM-15405	Indication of secure client communication with main server	A 5620 SAM GUI client that communicates with a main server over a secure channel displays a padlock icon in the login form, GUI status bar, and information form.	*5620 SAM User Guide* *5620 SAM | 5650 CPAM Installation and Upgrade Guide*
SAM-16722	Support for IPv6 UDPTCP entries on CPM filters	The 5620 SAM supports configuring a IPv6 CPM filter entry that filters on UDPTCP headers.	*5620 SAM System Administrator Guide*
Map enhancements			
SAM-362	Create from Template option in service map	The right-click contextual menu in a service map allows template-based service object creation, depending on the templates that are bound to the service.	Chapter 6
5620 SAM system management enhancements			
SAM-1848	SNMP monitoring	The 5620 SAM supports the monitoring of a 5620 SAM station using native RHEL or Solaris SNMP functions.	*5620 SAM | 5650 CPAM Installation and Upgrade Guide*, for optional OS packages related to SNMP

(1 of 21)

Feature ID	Feature or function	Description	See
SAM-19187	Windows support for client delegate server deployment	5620 SAM client delegate server deployment is supported on a Microsoft Windows platform for remote GUI client access.	*5620 SAM Planning Guide*, for platform and remote access requirements *5620 SAM | 5650 CPAM Installation and Upgrade Guide*, for configuration information
SAM-17345	Export of multiple script test results	The 5620 SAM supports the export of multiple script test results.	*5620 SAM Scripts and Templates Developer Guide*
SAM-19171	Database error monitoring	You can configure the 5620 SAM to raise an alarm when the Oracle database software detects an error. This function enhances troubleshooting and security by providing early notification of potential problems such as SQL injection attacks.	*5620 SAM System Administrator Guide*
SAM-19174	Configurable database login security	To increase database security, you can configure the 5620 SAM to limit the number of Oracle database login failures. When the specified limit is reached, the 5620 SAM prevents further database login attempts until the user account is unlocked.	*5620 SAM System Administrator Guide*
SAM-19361	One-time password use for remote users	You can enable one-time password use for RADIUS and TACACS+ during 5620 SAM remote authentication policy configuration.	*5620 SAM System Administrator Guide*
SAM-14940	NE resync audit	You can perform NE resync audits and identify configuration differences between managed NEs and the 5620 SAM database.	*5620 SAM Troubleshooting Guide*
Device management enhancements			
SAM-15929	Reserved blocks/IP addresses per ISA-NAT MDA	You can display the number of reserved port blocks and reserved IP addresses on an ISA-NAT MDA.	Procedure 24-6
SAM-17483	EMS definition in equipment tree	The 5620 SAM supports the categorization of an EMS within a created topology group.	Procedure 10-6
7210 SAS-D enhancements			
SAM-1249	Fault propagation for Epipe services	The 5620 SAM supports fault propagation for MEPs in VLL Epipe services for the 7210 SAS-D, Release 5.0 R2 or later.	Procedure 78-1
SAM-8345	IEEE 1588-2008 PTP timing synchronization	The 5620 SAM supports the configuration of an IEEE 1588-2008 PTP clock as the timing synchronization reference for the 7210 SAS-D 6F 4T ETR, Release 5.0 R2 or later.	Procedures 15-7, 15-14, and 15-15
SAM-14715	Transit service	The 5620 SAM supports transit services on VPLS and VLL services. For VPLS on G.8032 Ethernet rings you can use the Create Transit Service function. For VPLS and VLL services on non-G.8032 ring topologies, the 5620 SAM uses a manually-configured transit service. The 5620 SAM supports this feature for the 7210 SAS-D, Release 4.0 R7 or later.	Section 27.3 Procedure 27-10
SAM-15416	Up MEPs for VPLS	The 5620 SAM supports up MEPs for VPLS on the 7210 SAS-D, Release 5.0 R1 or later.	Procedures 68-21, 68-37, and 78-1

(2 of 21)

Feature ID	Feature or function	Description	See
SAM-15424	Fan support	The 5620 SAM supports the configuration of the fan administration mode for the 7210 SAS-D 128 Mbyte variant, Release 5.0 R2 or later.	Procedure 15-19
SAM-15835	EFM timing enhancements	When you configure ports for EFM OAM the 5620 SAM supports a minimum transmit interval of 100 ms (formerly 500 ms) for the 7210 SAS-D, Release 5.0 R2 or later.	Procedure 32-42
SAM-19336	IPv6 MAF support	The 5620 SAM extends support for IPv6 match criteria for management access filters to the 7210 SAS-D, Release 5.0 R1 or later. This feature is now supported on all 7210 SAS chassis types, Release 5.0 R1 or later.	*5620 SAM System Administrator Guide*
SAM-21667	Forwarding class and profile for mirror services	The 5620 SAM supports the configuration of forwarding classes and profiles for mirror services on the 7210 SAS-D, Release 5.0 R1 or later.	Procedure 69-2
7210 SAS-E enhancements			
SAM-15420	USB support (Sandisk 4Gb and 8Gb only)	The 5620 SAM supports USB devices as flash memory for storing accounting statistics for the 7210 SAS-E, Release 5.0 R2 or later.	*5620 SAM Statistics Management Guide*
SAM-15833	IPv6 ingress ACLs for VPLS and VLL services	The 5620 SAM supports IPv6 ingress ACL filter policies for the 7210 SAS-E Release 5.0 R3 or later, in VPLS and VLL services. Policies are supported on the 7210 SAS-E when the system resource profile is appropriately configured.	Procedures 13-20, 67-27, and 68-24 Chapter 8
SAM-19334	MVR support in VPLS	The 5620 SAM extends support for MVR configuration in VPLS services to the 7210 SAS-E, Release 5.0 R1 or later.	Procedures 68-17 and 68-35
SAM-19336	IPv6 MAF support	The 5620 SAM extends support for IPv6 match criteria for management access filters to the 7210 SAS-E, Release 5.0 R1 or later. This feature is now supported on all 7210 SAS chassis types, Release 5.0 R1 or later.	*5620 SAM System Administrator Guide*
SAM-21667	Forwarding class and profile for mirror services	The 5620 SAM supports the configuration of forwarding classes and profiles for mirror services on the 7210 SAS-E, Release 5.0 R1 or later.	Procedure 69-2
7210 SAS-M enhancements			
SAM-1249	Fault propagation for Epipe services	The 5620 SAM supports fault propagation for MEPs in VLL Epipe services for the 7210 SAS-M, Release 5.0 R2 or later.	Procedure 78-1
SAM-8339	Up MEPs for Epipe and VPLS	The 5620 SAM supports up MEPs for Epipe and VPLS services on the 7210 SAS-M (in access uplink mode), Release 5.0 R2 or later.	Procedures 68-21, 68-37, and 78-1
SAM-10062	IPv6 support for IS-IS	The 5620 SAM supports IPv6 addressing during IS-IS configuration for the 7210 SAS-M, Release 5.0 R2 or later.	Procedure 23-20
SAM-14715	Transit service	The 5620 SAM supports transit services on VPLS and VLL services. For VPLS on G.8032 Ethernet rings you can use the Create Transit Service function. For VPLS and VLL services on non-G.8032 ring topologies, the 5620 SAM uses a manually-configured transit service. The 5620 SAM supports this feature for the 7210 SAS-M (in access-uplink mode), Release 4.0 R7 or later.	Section 27.3 Procedure 27-10

(3 of 21)

Feature ID	Feature or function	Description	See
SAM-15418	Processing of 3-plus-tag packets received on a QinQ SAP in an Epipe service	The 5620 SAM supports the configuration of a dot1q or QinQ L2 access interface on 3-plus-tag Epipe services for the 7210 SAS-M, Release 5.0 R2 or later. A 3-plus-tag Epipe service preserves customer tags when packets received on a QinQ SAP are forwarded to a spoke SDP binding or a dot1q or QinQ L2 access interface.	Section 67.1 Procedures 67-2, 67-4, and 67-27
SAM-15420	USB support (Sandisk 4Gb and 8Gb only)	The 5620 SAM supports USB devices as flash memory for storing accounting statistics for the 7210 SAS-M, Release 5.0 R2 or later.	*5620 SAM Statistics Management Guide*
SAM-15835	EFM timing enhancements	When you configure ports for EFM OAM the 5620 SAM supports a minimum transmit interval of 100 ms (formerly 500 ms) for the 7210 SAS-M, Release 5.0 R2 or later.	Procedure 32-42
SAM-21626	Processing of 3-plus-tag packets in QinQ to QinQ traffic	The 5620 SAM supports the configuration of two QinQ L2 access interfaces on 3-plus-tag Epipe services for the 7210 SAS-M, Release 5.0 R3 or later. A 3-plus-tag Epipe service preserves customer tags when packets received on a QinQ SAP are forwarded to a spoke SDP binding or a dot1q or QinQ L2 access interface.	Section 67.1 Procedures 67-2, 67-4, and 67-27
SAM-21628	Ethernet CFM support in 3-plus-tag Epipe services	The 5620 SAM supports Ethernet CFM on 3-plus-tag Epipe services for the 7210 SAS-M, Release 5.0 R3 or later.	Section 67.1
SAM-21667	Forwarding class and profile for mirror services	The 5620 SAM supports the configuration of forwarding classes and profiles for mirror services on the 7210 SAS-M, Release 5.0 R1 or later.	Procedure 69-2
7210 SAS-X enhancements			
SAM-1249	Fault propagation for Epipe services	The 5620 SAM supports fault propagation for MEPs in VLL Epipe services for the 7210 SAS-X, Release 5.0 R2 or later.	Procedure 78-1
SAM-15422	IEEE 1588-2008 PTP timing synchronization	The 5620 SAM supports the configuration of an IEEE 1588-2008 PTP clock as the timing synchronization reference for the 7210 SAS-X, Release 5.0 R3 or later.	Procedures 15-7, 15-14, and 15-15
SAM-10062	IPv6 support for IS-IS	The 5620 SAM supports IPv6 addressing during IS-IS configuration for the 7210 SAS-X, Release 5.0 R2 or later.	Procedure 23-20
SAM-15418	Processing of 3-plus-tag packets received on a QinQ SAP in an Epipe service	The 5620 SAM supports 3-plus-tag Epipe services on the 7210 SAS-X, Release 5.0 R2 or later. A 3-plus-tag Epipe service preserves customer tags when packets received on a QinQ SAP are forwarded to a spoke SDP binding or a dot1q or QinQ L2 access interface.	Section 67.1 Procedures 67-2, 67-4, and 67-27
SAM-15835	EFM timing enhancements	When you configure ports for EFM OAM the 5620 SAM supports a minimum transmit interval of 100 ms (formerly 500 ms) for the 7210 SAS-X, Release 5.0 R2 or later.	Procedure 32-42
SAM-21626	Processing of 3-plus-tag packets in QinQ to QinQ traffic	The 5620 SAM supports the configuration of two QinQ L2 access interfaces on 3-plus-tag Epipe services for the 7210 SAS-X, Release 5.0 R3 or later. A 3-plus-tag Epipe service preserves customer tags when packets received on a QinQ SAP are forwarded to a spoke SDP binding or a dot1q or QinQ L2 access interface.	Section 67.1 Procedures 67-2, 67-4, and 67-27
SAM-21628	Ethernet CFM support in 3-plus-tag Epipe services	The 5620 SAM supports Ethernet CFM on 3-plus-tag Epipe services for the 7210 SAS-X, Release 5.0 R3 or later.	Section 67.1

(4 of 21)

Feature ID	Feature or function	Description	See
SAM-21667	Forwarding class for mirror services	The 5620 SAM supports the configuration of forwarding classes for mirror services on the 7210 SAS-X, Release 5.0 R1 or later.	Procedure 69-2
7450 ESS and 7750 SR enhancements			
	New daughter card support	The 5620 SAM supports the following new daughter cards: • 2-Port 10GE MDA with WaveTracker • 1-port 100GE, 10-port GE Combo Plasma IMM on the 7750 SR-7, 7750 SR-12, and 7750 SR-12E • FP3 1-Port 100GE DWDM IMM on the 7750 SR-12 and 7750 SR-12E	Chapter 15
SAM-12813	Soft reset support for FP3-based line cards	The 5620 SAM supports performing a soft reset on FP3-based line cards installed in a Release 11.0 R1 or later 7450 ESS or 7750 SR.	*5620 SAM System Administrator Guide*
SAM-12819	Mixed-mode ISA support	The 5620 SAM supports configuring the following objects on a mixed-mode 7450 ESS or 7750 SR, Release 11.0 or later: • ISA broadband applications, ISA video, and ISA tunnel daughter cards • VSM-CCA cards • ISA LNS groups • ISA NAT groups • ISA Tunnel groups • ISA Video groups • ISA WLAN GW groups (7750 SR only)	Chapter 14
SAM-13142	Synchronous ethernet with SSM support for 48-port 1GB Ethernet EPTX MDA.	The 5620 SAM supports configuring synchronous Ethernet with SSM on 48-port 1GB Ethernet Extended Performance TX MDAs on the 7750 SR.	Procedure 15-33
SAM-14509	TCA support for LAGs on 7450 ESS, 7710 SR, 7750 SR, and 7950 XRS	The 5620 SAM supports enabling TCA on LAG objects configured on 7450 ESS, 7710 SR, 7750 SR, and 7950 XRS nodes.	Section 14.10
SAM-15693	Support for IPv6 Cflowd collectors	The 5620 SAM supports configuring Cflowd collectors that use IPv6 addresses.	Procedure 13-5
SAM-18598	ISA-IPsec support on 7450 ESS in mixed mode	The 7450 ESS in mixed mode provides the same IPsec support as the 7750 SR.	—
SAM-18661	Support for coherent optical configuration	The 5620 SAM supports configuring coherent optical parameters on the Ethernet port of a 1-Port 100GE OTU4 DWDM tunable optic IMM.	Procedure 16-1
SAM-21031	NTP support on 7750 SR	The 5620 SAM supports configuring NTP on the 7750 SR, and on VPRN sites located on the 7750 SR.	Procedures 15-10 and 71-23
7705 SAR enhancements			
SAM-5834	APS on 2P OC3 access side	The 5620 SAM supports the configuration of SC APS on a 2-port OC3 MDA on the 7705 SAR-8 and 7705 SAR-18, Release 6.0 R1 or later.	Chapters 16 and 34
SAM-5836	CSMv2 card support	The 5620 SAM supports the configuration of a CSMv2 card on the 7705 SAR-8.	Section 8.9
SAM-5838	2 port ring MDA support	The 5620 SAM supports the configuration of a 2 × 10-Gig Bridged Ethernet XFP + 1 × 2.5G Virtual Ethernet card on the 7705 SAR-8 and 7705 SAR-18, Release 6.0 R1 or later.	Section 8.9 Procedures 15-33, 16-1, 16-17, and 43-6

(5 of 21)

Feature ID	Feature or function	Description	See
SAM-5840	Multi-chassis LAG support	The 5620 SAM supports MC LAG groups on the 7705 SAR-8, 7705 SAR-18, 7705 SAR-A, 7705 SAR-M and 7705 SAR-W, Release 6.0 R1 or later.	Sections 8.9, 36.1, and 39.1
SAM-5843	Multi-chassis APS support	The 5620 SAM supports multi-chassis APS on the 7705 SAR, Release 6.0 R1 or later.	Section 34.1
SAM-5845	PIM support	The 5620 SAM supports the enabling and configuration of PIM on a routing instance on the 7705 SAR, Release 6.0 R1 or later.	Procedures 23-39, 23-40 and 23-43
SAM-5847	Multicast protocol support	The 5620 SAM supports multicast protocols on the 7705 SAR, Release 6.0 R1 or later.	Chapter 23
SAM-5849	MLD support	The 5620 SAM supports configuration of MLD in a multicast domain on the 7705 SAR, Release 6.0 R1 or later.	Sections 23.1 and 61.2
SAM-5857	8-port FXO Adapter card support	The 5620 SAM supports the configuration of an 8-port FXO Adapter card on the 7705 SAR-8 and the 7705 SAR-18, Release 6.0 R1 or later.	Section 8.9
SAM-10069	Remove a PPP link from an MLPPP bundle	The 5620 SAM supports the automatic removal of a PPP link from an MLPPP bundle if the DS1 BER exceeds a threshold on the 7705 SAR, Release 5.0 R5 or later.	Procedures 15-41 and 16-33
SAM-11303	LDP prefix-aggregation	The 5620 SAM supports the introduction of LDP prefix-aggregation on the 7705 SAR, Release 6.0 R1 or later.	Section 23.18 Procedure 23-17
SAM-11307	VRRP support	The 5620 SAM supports VRRP on IES and VPRN services with policies and router interfaces on the 7705 SAR, Release 6.0 R1 or later.	Procedures 70-40 and 71-42
SAM-11309	BFD 10-ms timer	The 5620 SAM supports BFD transmitter and receiver values from 10 milliseconds to 100 000 milliseconds on the 7705 SAR, Release 6.0 R1 or later.	Procedure 22-10
SAM-11311	Routed VPLS to IES/VPRN	The 5620 SAM supports the routed VPLS connector function on the 7705 SAR, Release 6.0 R1 or later.	Section 74.1 Procedures 70-19 and 71-30
SAM-11315	Port-level hard policing at SAP ingress	The 5620 SAM supports port-level hard policing at the SAP ingress for the 7705 SAR, Release 6.0 R1 or later.	Procedure 16-1
SAM-11317	MEF 8 support on Epipe services	The 5620 SAM supports MEF 8 on Epipe services for the 7705 SAR, Release 6.0 R1 or later. MEF 8 allows TDM services to be emulated across Epipe services using circuit emulation.	Section 67.1 Procedure 67-27
SAM-11325	2-port ring MDA SFP support	The 5620 SAM supports SFP on the 2-port ring MDA, enabling the Media Adapter and DDM tabs at the port level on the 7705 SAR-8 and the 7705 SAR-18, Release 6.0 R1 or later.	Section 8.9 Procedure 16-1
SAM-11327	LDP LSR ECMP support	The 5620 SAM supports the configuration of ECMP on an LDP routing interface, on the 7705 SAR, Release 6.0 R2 or later.	Procedures 23-17 and 32-29
SAM-11329	RIP routing site support	The 5620 SAM supports a RIP routing site in the routing navigation tree on the 7705 SAR, Release 6.0 R1 or later.	Section 23.17 Procedures 23-9, 23-10, and 23-11
SAM-11333	7705 SAR-W support	The 5620 SAM supports the introduction of the 7705 SAR-W.	Section 8.9 Procedure 15-36

(6 of 21)

Feature ID	Feature or function	Description	See
SAM-12363	NTP support	The 5620 SAM supports NTP on the 7705 SAR, Release 5.0 R5 and 6.0 R1 or later. The 7705 SAR acts only as an NTP client.	Procedure 15-10
SAM-13172	Differential clock on ASAP v2	The 5620 SAM supports the configuration of a differential clock on 16/32x channelized ASAP v2 cards on the 7705 SAR-8 and 7705 SAR-18, Release 6.0 R1 or later.	Procedure 15-33
SAM-13174	SSM for E1 channels	The 5620 SAM supports the configuration of synchronous status messages on E1 channels on the 7705 SAR, Release 6.0 R1 or later. HSMs are used by synchronous Ethernet peers to ensure the quality of the timing synchronization source.	Procedure 16-31
SAM-13176	SAP down, MEP up	When you associate a MEP with an Epipe L2 access interface, you can configure the parameter Hold MEPs Up When SAP is Down so that if the SAP is down, the MEP remains operationally up, on the 7705 SAR, Release 6.0 R1 or later.	Procedure 67-34
SAM-13791	9500 MPRe integration	The 5620 SAM supports the integration of the 9500 MPRe on the 7705 SAR-8 and 7705 SAR-18 as a single NE, Release 6.0 R1 or later. The configuration of radio parameters is via the MCT tool. Management capabilities provide radio discovery, configuration status and state, alarm integration and management, and statistics management. MPT software packages are bundled with the 7705 SAR image and the files are pushed to the 7705 SAR during a 5620 SAM upgrade.	Procedures 15-12 and 67-27 *5620 SAM System Administrator Guide*
SAM-13793	9500 MPRe integration	The 5620 SAM supports the integration of the 9500 MPRe on the 7705 SAR-8 and 7705 SAR-18 as a single NE, Release 6.0 R1 or later. Radio links between an integrated single NE are discovered and displayed on the 5620 SAM physical map. All link-related faults are correlated to ports and to upper layer objects like LSPs or services.	Procedure 15-12
SAM-13857	9500 MPRe integration	The 5620 SAM supports an integrated MCT cross-launch from the NE or port level on the 7705 SAR-8 and 7705 SAR-18 as a single NE, Release 6.0 R1 or later.	–
SAM-13874	7705 SAR-A support	The 5620 SAM supports the introduction of the 7705 SAR-A.	Section 8.9
SAM-13986	SAP aggregation group topology map enhancements	SAP aggregation groups are displayed in the topology map view and navigation tree for VLL Apipe services.	Procedure 67-52 Section 6.2
SAM-15409	SAP egress support	The 5620 SAM supports SAP egress support on the 7705 SAR, Release 6.0 R1 or later.	Section 43.1 Procedure 43-26
SAM-15447	Scheduled statistics support for SNMP-based counters	The 5620 SAM supports the enabling of SNMP-based scheduled statistics for Port Net Egress accounting statistics on the 7705 SAR.	*5620 SAM Statistics Management Guide*
SAM-15708	CFM synthetic loss measurement test support	The 5620 SAM supports CFM two-way SLM tests for Epipe services on the 7705 SAR, Release 6.0 R1 or later.	Section 32.1
SAM-15710	7705 SAR DHCP client on the network interface	The 5620 SAM supports the DHCP client on the network interface on the 7705 SAR.	Procedure 22-10

(7 of 21)

Feature ID	Feature or function	Description	See
SAM-15714	GPON module SFP support	The GPON module card supports SFP on the 7705 SAR-M Release 6.0 R1 or later, enabling the Media Adapter and DDM tabs at the port level.	Section 8.9 Procedure 16-1
SAM-15722	IPv6 support for 4-port OC3	The 5620 SAM supports the configuration of IPv6 interfaces on ports on the 4-port OC3/STM1 ASAP SFP card.	Procedure 16-1
SAM-15848	STM1 Electrical 0/70C SFP support	The 2-port OC3/STM1 ASAP SFP card supports the STM1 Electrical 0/70C SFP on the 7705 SAR-8 and the 7705 SAR-18, Release 5.0 R6 or later.	Section 16.2
SAM-15903	OAM test enhancement for DSL modules	F5 OAM loopback test added to the ATM services. This test can also be executed from a test suite.	Section 32.1 Procedure 32-22
SAM-16224	Differential clock on 4p DS3/E3	The 5620 SAM supports the configuration of a differential clock on a 4 × channelized DS3/E3 ASAP on the 7705 SAR-8, 7705 SAR-18, 7705 SAR-A and 7705 SAR-W.	Procedures 15-33, 16-31, and 16-34
SAM-16314	ICB on MC LAG support	The 5620 SAM supports the configuration of ICB on MC LAG for Epipe services on the 7705 SAR, Release 6.0 R1 or later.	Section 39.1 Procedure 67-4
SAM-17875	OAM tests for multicast protocols	The 5620 SAM supports multicast router information, OAM diagnostics and multicast trace OAM diagnostics on the 7705 SAR, Release 6.0 R1 or later.	Procedures 32-30 and 32-31
7705 SAR-H enhancements			
SAM-11045	7705 SAR-H License	The 5620 SAM supports licenses for 7705 SAR-H firewall features. It provides a count of software licenses for firewall on the 7705 SAR platform. It also provides standard 5620 SAM provisioning and assurance features.	*5620 SAM System Administrator Guide*
SAM-11057	7705 SAR-H Firewall—Host Group policy	The 5620 SAM supports the configuration of a Host Group firewall policy on the 7705 SAR-H.	Procedure 60-1
SAM-11061	7705 SAR-H Firewall manager	The 5620 SAM supports the 7705 SAR-H firewall features through a centralized firewall manager. You can allow zone definition entries to be applied to the firewall by using the management access interface and the CPM interface.	*5620 SAM System Administrator Guide*
SAM-11063	7705 SAR-H Firewall—Service Group policy	The 5620 SAM supports the configuration of a Service Group firewall policy on the 7705 SAR-H.	Procedure 60-2
SAM-11065	7705 SAR-H Firewall—Rule Set policy	The 5620 SAM supports the configuration of a Rule Set firewall policy on the 7705 SAR-H.	Procedure 60-3
SAM-11068	7705 SAR-H Firewall—Zone policy	The 5620 SAM supports the configuration of a Zone firewall policy on the 7705 SAR-H.	Procedure 60-4
SAM-11093	7705 SAR-H Firewall—Zone management	The 5620 SAM supports firewalls in zones to set a level of trust and access rights to a set of related objects like interfaces, host addresses, and users on the 7705 SAR-H.	Section 60.1
SAM-11760	7705 SAR-H firewall statistics	The 5620 SAM supports firewall statistics provided by the firewall at the firewall site, zone, SAP, Spoke-SDP, management access firewall and CPM firewall.	*5620 SAM Statistics Management Guide*
SAM-11762	7705 SAR-H firewall alarms	The 5620 SAM supports firewall alarms on the 7705 SAR-H.	*5620 SAM Alarm Reference*

(8 of 21)

Feature ID	Feature or function	Description	See
SAM-11783	7705 SAR-H combo MDA	The 5620 SAM supports combo MDAs on the 7705 SAR-H.	Section 8.9
SAM-11769	7705 SAR-H system and services	The 5620 SAM supports the following services/pseudowires on the 7705 SAR-H: • VLL (Cpipe, Epipe, Ipipe) • VPRN • IES • VPLS The 5620 SAM does not support the following VLL services in Release 11.0R1: • Apipe • Fpipe • Hpipe The 5620 SAM supports the following network management functions on the 7705 SAR-H: • Backup and Restore • Software Upgrade • IPv6 • SNMPv3 • Routing	Chapters 67, 68, 70, 71, 9, 10, 22, 23, 71
SAM-11771	7705 SAR-H QoS policy	The 5620 SAM supports QoS policies on the 7705 SAR-H: • Access ingress policy • Access egress policy • MC MLPPP egress QoS profiles • Network policy • Network queue policies • Slope policies	Table 42-1 Chapter 43
SAM-11773	7705 SAR-H network synchronization	The 5620 SAM supports the configuration of an IEEE 1588-2008 PTP clock as the timing synchronization reference for the 7705 SAR-H. The 5620 SAM supports the following features on network synchronization. • IEEE 1588-2008 PTP timing synchronization • Time of Day	Chapters 15 and 46 Procedures 15-7, 15-8, and 15-9
SAM-11775	7705 SAR-H PoE	The 5620 SAM supports internal and external PoE on the 7705 SAR-H.	Section 15.4 Procedure 16-19

SAM-11777	7705 SAR-H OAM	The 5620 SAM supports the following OAM functionality on the 7705 SAR-H:
		• ICMP ping
		• MAC trace OAM
		• MAC ping OAM
		• LSP ping OAM
		• LSP trace OAM
		• MAC purge OAM
		• MAC populate OAM
		• CFM Eth test diagnostic
		• CFM one-way delay
		• CFM two-way delay
		• NE schedulable OAM tests
		• Non-NE schedulable OAM tests
		• Service Test Manager
		  • Test policies
		  • Test suites
			Sections 32.1 and 77.1
			Procedures 32-9, 32-10, 32-11, 32-46, and 32-47

(9 of 21)

Feature ID	Feature or function	Description	See
SAM-11767	7705 SAR-H compact MDA	The 5620 SAM supports compact MDAs on the 7705 SAR-H. Power supply source is supported on the 7705 SAR-H.	Sections 8.9 Chapter 16 Procedures 15-33, 16-1, 16-11, 16-12, 16-27, 16-32, and 16-33
SAM-20826	7705 SAR-H DHCP server support	The 5620 SAM supports configuring local DHCP servers on the 7705 SAR-H on VPRN and Routing Interfaces. The local DHCP server leases IP addresses to clients in the network.	Chapters 22, 65, and 71 Procedures 22-2 and 22-10
7950 XRS enhancements			
SAM-14417	Support for static pseudowire routing	The 5620 SAM supports static pseudowire routing on the 7950 XRS, Release 11.0 R1 or later.	Section 72.1
SAM-14426	Support for VLL Ipipe services	The 5620 SAM supports the creation of VLL Ipipe services on the 7950 XRS-20.	Procedure 67-18
SAM-18375 SAM-18373	400 GE XMA cards	The 5620 SAM supports the configuration of the following 400 GE XMA cards for the 7950 XRS-20: • 40-port 10 GE SFP+ XMA • 4-port 100 GE CXP XMA	Procedure 15-23 Section 8.16
SAM-19081	SFM X20 B cards	The 5620 SAM supports the configuration of SFM X20 B cards in SFM card slots on the 7950 XRS-20.	Procedure 15-23 Section 8.16
9500 MPR/9500 MPRe enhancements			
—	9500 MPRe integration with 7705 SAR	See SAM-13791, SAM-13793, and SAM-13857 for feature details.	—
OmniSwitch enhancements			
SAM-5565	OS 6900 and OS 10K AOS 7.3.1 support	The 5620 SAM supports the AOS Release 7.3.1 or later on the OS 6900 and OS 10K switches.	Section 8.21
SAM-8475	OS 6900 and OS 10K MC AOS group support	The 5620 SAM supports the configuration of MC AOS groups on the OS 6900 and OS 10K NEs, Release 7.3.1 or later. This includes the creation of MC AOS LAG groups, MC AOS VFLink groups, IPC VLANs, and VIP VLANs.	Procedure 39-5, 39-6, 39-7, 39-8, and 66-4
SAM-8850 SAM-10678	Additional cards supported on OS 10K	The 5620 SAM supports OS10K-QNI-U4, OS10K-QNI-U8, and OS10K-XNI-U16E cards on OS 10K switches.	Section 8.21
SAM-8854 SAM-8857 SAM-8995	OS 6900 and OS 10K Ethernet OAM and SAA support	The 5620 SAM supports the use of the Service Test Manager for Ethernet OAM and SAA activities on the OS 6900 and OS 10K NEs, Release 7.3.1 or later.	Chapter 32, 77 and 78
SAM-14691	OS 6400, OS 6850E, OS 6855, OS 9700E, and OS 9800E AOS 6.4.5 support	The 5620 SAM supports the AOS Release 6.4.5 or later on the OS 6400, OS 6850E, OS 6855, OS 9700E, and OS 9800E switches.	Section 8.21
SAM-14693	Extended CPE test-head support	The 5620 SAM supports the configuration of CPE SLA test-head OAM tests on the OS 6850, OS 6855 U24X, and OS 9000E NEs.	Section 77.11
SAM-15526	OS 6850E and OS 6855 Dying Gasp support	The 5620 SAM supports Dying Gasp - Power Loss on the OS 6850E and OS 6855 NEs, Release 6.4.5 or later.	Procedure 13-26
SAM-15550 SAM-15564	Custom L2 profiles	The 5620 SAM supports the creation of custom L2 profiles on the OS 6250M, OS 6450, and OS 6850E NEs.	Procedure 52-3

(10 of 21)

Feature ID	Feature or function	Description	See
Network management enhancements			
SAM-335	Normalized Statistics Plotter graphs	You can use the 5620 SAM Statistics Plotter to plot octet throughput as a calculated bit rate using a specified scale, such as Gb/s.	*5620 SAM Statistics Management Guide*
SAM-844	Incongruent routing topology for VPRN	The 5620 SAM supports configuring static routes and BGP, OSPF and PIM sites on a VPRN to use separate routing tables for unicast and multicast traffic.	Procedure 71-12 Procedure 71-50
SAM-8211	Additional text policies	The 5620 SAM supports additional text policies to display specific information about an alarmed object in the additional text column of the dynamic alarm list and on the Alarm Info form.	Procedure 31-5
SAM-8571	NAT configuration usability	Reorganization of NAT configuration GUI with usability enhancements.	Chapter 24
SAM-9614	RHEL support for 3GPP OSS interface	The 3GPP OSS interface is supported for 5620 SAM systems on RHEL.	*5620 SAM | 5650 CPAM Installation and Upgrade Guide*
SAM-12038 SAM-2752	IPsec multi-chassis redundancy	5620 SAM MC IPsec redundancy provides a one-to-one inter-NE stateful failover mechanism for IPsec tunnels. MC IPsec provides protection for NE failure or MS-ISA failure. This feature supports only IKEv2 static LAN-to-LAN tunnels on multi-active tunnel groups.	Section 29.3
SAM-12889	MAC accounting	The 5620 SAM supports the collection of statistics for MAC address traffic on the following L3 interfaces: • Network interface • IES SAP • VPRN SAP	Procedures 22-9, 70-17, and 71-22
SAM-12894	Indirect next-hop for route aggregation	The 5620 SAM supports creating a route aggregation with an indirect IP address as the next-hop.	Procedure 71-21
SAM-12966	Unnumbered L3 network interfaces for MPLS	The 5620 SAM supports the selection of an unnumbered L3 network interface on MPLS interfaces. Unnumbered L3 network interfaces do not have an IP address configured.	Procedure 25-3
SAM-12982	One-second CCM interval	The 5620 SAM supports setting the CCM interval for ethernet rings to 1s.	Procedures 27-6 and 78-1
	G.8032 support for 7450 ESS-6, 7750 SR-c4, and 7750 SR-c12	The 5620 SAM supports configuring G.8032 ethernet ring elements and global MEGs on the 7450 ESS-6, 7750 SR-c4, and 7750 SR-c12. For these platforms, the CCM interval must be set to 1s.	
SAM-13034	Distributed CPU protection	An NE DDoS protection policy extends DoS protection functionality by controlling traffic destined to IOM or CPM CPUs on a per SAP, per protocol basis. A DDoS protection policy can be configured on a base router network interface, as well as on a variety of VPRN, IES, VPLS, and VLL SAPs.	*5620 SAM System Administrator Guide* Chapters 22, 67, 68, 70, and 71
SAM-13088	Deterministic NAT	Support for deterministic NAT configuration on a base routing instance, and on a VPRN routing instance.	Chapter 24 Procedure 24-3
SAM-13102	Migrant user handling	Support for migrant user handling in a Wi-Fi offload application through IES and VPRN soft GRE group interfaces.	Chapter 35 Procedures 71-62 and 70-13

(11 of 21)

Feature ID	Feature or function	Description	See
SAM-14176	RADIUS CoA port	The 5620 SAM supports the system-wide configuration of the RADIUS CoA port on an NE.	Procedure 13-17
SAM-14278	Custom text for alarm policies	The 5620 SAM supports up to 256 characters of custom text that can be added to an alarm policy.	Procedure 31-2
SAM-14679	Dual sided plotter infrastructure	By clicking on a button, you can plot statistics for the other endpoint of an object such as a physical or an optical link that terminates on a physical port.	*5620 SAM Statistics Management Guide*
SAM-15306	Set OLC state when shutting down or turning up an object	The 5620 SAM supports setting the OLC state of an object to Maintenance when an object is shut down or In Service when an object is turned up using the System Preferences form.	*5620 SAM System Administrator Guide*
SAM-15355	Statistics Plotter Improvements: save option	The monitored object name is displayed in the legend of the 5620 SAM Statistics Plotter when the Legend option is selected. The object name is also shown in a saved view of a graph when the option is selected.	*5620 SAM Statistics Management Guide*
SAM-15645	Post-discovery auto-configuration	In a 5620 SAM discovery rule, you can specify a post-discovery action to perform on successfully discovered NEs after rule execution. A post-discovery action is a 5620 SAM control script that invokes other control or XML API scripts to send configuration information to the discovered NEs.	Chapter 10 *5620 SAM Scripts and Templates Developer Guide*
SAM-15708	Egress hash configuration support for LAG access	Support for configuring a LAG group to use per-link egress hashes for LAG access eligibility.	Procedure 14-10
SAM-15827	NAT44 efficiency improvements	Support for on-demand retrieval of large-scale NAT entries, based on a routing instance ID.	Procedure 24-7
SAM-16007	Extended hardware virtualization support	Live network deployment of a 5620 SAM main server, database, or auxiliary server in a VM is supported.	*5620 SAM Planning Guide* *5620 SAM | 5650 CPAM Installation and Upgrade Guide*
SAM-16572	Control script input from file	A 5620 SAM control script can import information from a local or remote text or XML file.	*5620 SAM Scripts and Templates Developer Guide*
SAM-17978	Additional columns in the Historical Alarms list	The 5620 SAM supports the following additional columns in the Historical Alarms form: • Previous Severity • Original Severity • Highest Severity • Last Time Severity Changed • Last Time Cleared	Procedure 3-30
SAM-18618	WebDAV configuration during 5620 SAM installation or upgrade	You can enable or disable WebDAV access to activation data during a 5620 SAM main server installation or upgrade. The WebDAV access setting persists through subsequent upgrades.	*5620 SAM | 5650 CPAM Installation and Upgrade Guide*
SAM-18828	Real-time plotting for dynamic objects	You can plot LSN subscriber host statistics data using the 5620 SAM Statistics Plotter.	Procedure 24-9
SAM-19019	Node redundancy on PW ports	Support for MC sync group configuration on PW ports for ESM over MPLS Pseudowire redundant configurations.	Procedure 16-13
SAM-19369	UDP authentication and accounting ports	Support for UDP authentication port and UDP accounting port configuration on a RADIUS server site on a routing instance.	Procedure 22-7

(12 of 21)

Feature ID	Feature or function	Description	See
SAM-19406	Multiple control-script instances	The 5620 SAM Script Manager supports the creation of multiple control-script instances, as is done for XML API scripts. The script instances and results are stored in the 5620 SAM database.	*5620 SAM Scripts and Templates Developer Guide*
Protocol enhancements			
SAM-12891	BGP flowspec support	The 5620 SAM supports the following BGP flowspec enhancements: • IPv6 • VPRN BGP for the flowspec IPv4 and IPv6 address families on PE-CE eBGP and PE-PE iBGP sessions • flowspec filtering on VPRN IP interfaces • flowspec filtering on IES IP interfaces	Procedures 22-10, 23-2, 23-4, 23-5, 70-8, 70-17, 71-22, and 71-56
SAM-12895	BGP Routing Policy Support	The 5620 SAM supports using routing policies for BGP next hop resolution and peer tracking. Applying a routing policy to a BGP restricts which routes are considered valid when determining a path to a peer or next hop.	Procedure 23-2
SAM-12913	Filter out LSA on OSPF instances	The 5620 SAM supports filtering out flooded LSAs on an OSPF interface. The filter can be configured to block all flooded LSAs, or to allow LSAs from the router or type 3, 5, or 7 default LSAs.	Procedure 23-27
SAM-12900 SAM-12901	Multiple OSPFv3 instance support	The 5620 SAM supports configuring multiple OSPFv3 instances on router instances and routing interfaces.	Section 23.20
SAM-12903	IPv4 address family support on OSPFv3	The 5620 SAM supports configuring OSPFv3 instances that support IPv4 addresses. OSPFv3 instances configured with an Instance ID of 0 to 31 support IPv6, and 64 to 95 support IPv4.	Section 23.20
SAM-12927	Accumulated IGP support	The 5620 SAM supports using accumulated IGP metrics with BGP peer groups, peers, and routing policy statements.	Procedure 23-4, 23-5, and 22-15
SAM-12933	Multicast fast-failover	You can enable fast failover on multicast IP streams on PIM interfaces.	Procedure 23-40
SAM-12950	Automatic ABR selection for inter-area RSVP P2P LSP	The 5620 SAM extends the existing behavior by making the ABR selection automatic at the ingress LER. You do not need to include the ABR as a loose hop in the LSP path definition.	Automatic ABR selection and dynamic ABR bypass protection Procedure 25-22
	Dynamic Bypass LSP for ABR NE protection	The 5620 SAM supports dynamic bypass computation, signaling, and association with the primary path of an inter-area P2P LSP to provide ABR NE protection.	Dynamic bypass LSP for ABR NE protection
SAM-12958	T-LDP hello reduction	The 5620 SAM supports hello reduction for target peers in an LDP session.	Procedures 23-13 and 23-16
SAM-12972	Administrative group support on FRR backup LSP	The administrative group constraints configured on an LSP primary path are used for the signalling of bypass LSPs. Both the P2P LSP and the P2MP S2L path bypass LSPs are supported.	Procedures 25-2, 25-8, 25-9, 25-13, and 25-23
SAM-12976	LDP support loopback interface as LSR-ID	The 5620 SAM supports the selection of any local loopback interface as the local LSR-ID during LDP interface creation.	Procedure 23-14
SAM-13016	Sender-only and receiver-only MVPN	The 5620 SAM supports the configuration of sender-only, receiver-only, and sender-and-receiver MVPN for PIM.	Procedure 23-40

(13 of 21)

Feature ID	Feature or function	Description	See
SAM-13076	LAC parameter configuration at site level	You can configure LAC parameters at the L2TP site level. The parameters can be inherited by child L2TP tunnel group profiles and L2TP tunnel profiles.	Chapter 23 Procedure 23-34.
SAM-13547	LAC tunnel selection enhancements	A Tunnel Selection Blacklist function is configurable on L2TP sites. The function suspends tunnels that return predetermined result codes, indicating that they are inoperative.	Section 23.1 Procedure 23-34
	Cisco NAS-Port	Support for Cisco NAS-Port Ethernet and Cisco NAS-Port ATM configuration on an L2TP site. The parameters specify Cisco NAS-Port information to include in the Cisco NAS-Port AVP for L2TP control messages related to a session in an L2TP protocol instance.	Procedure 23-34
SAM-14218	IGP shortcut relative metric support	The 5620 SAM supports LFA rule definitions and relative metric values for SPF calculation for IGP shortcuts.	Procedures 25-8 and 25-10
SAM-14224	Community for aggregate routes	The 5620 SAM supports assigning a community to an aggregate route on a base or VPRN routing instance.	Procedures 22-1 and 71-21
SAM-15690	Static route for BGP flap suppression	The 5620 SAM supports dynamic next-hop BGP route selection for black hole static routes on a base routing instance.	Procedure 22-13
SAM-15696	OSPF option to relax the condition that an ABR must have an adjacency in area 0 to advertise default into NSSA	A base router OSPF instance that is an ABR to an NSSA no longer must have a full adjacency in area 0 in order to advertise a default route into the NSSA. You can enable the Adjacency Check parameter to enforce an ABR to have an adjacency in area 0 before the default route or routes can be advertised into the NSSA.	Procedures 23-25 and 23-31
SAM-15917	Community for static routes	The 5620 SAM supports assigning a community to a static route on a base or VPRN routing instance.	Procedures 22-13 and 71-12
SAM-16739	Timer-based restart of BGP session when prefix limit reached	You can specify the maximum idle time during which BGP peering is disabled before there is an attempt to re-establish the connection with the BGP peer when the prefix limit is reached.	Procedures 23-4 and 23-5
	next-hop-self for VPN routes on a route reflector	You can configure the base router BGP instance to allow a route reflector of IP-VPN routes to use its IP address as the next hop rather than BGP choosing the next hop.	Procedure 23-2
	BGP local AS prepended to AS path	The 5620 SAM supports the option of prepending only the local AS to the AS path and not the global AS when routes are advertised to an eBGP peer that is configured for local AS.	Procedure 23-2, 23-4 and 23-5
SAM-16929	RFE 145092	Enhancement to weighted session assignment method. Next Attempt configuration on L2TP sites (base and VPRN routing instance) specifies how backup tunnels are chosen in the event of session failure.	Procedure 23-34
SAM-20304	Removal of LAG limitations for high-speed interfaces	The 5620 SAM supports a maximum reference bandwidth of up to 4 Tb/s on the following interfaces: • IS-IS instance • OSPF instance • OSPF3 instance • VPRN OSPF instance	Chapter 23
SAM-21151	RFE 141713	Configurable CHAP Challenge length on L2TP tunnel group profile and L2TP tunnel profile.	Procedure 23-34

(14 of 21)

Feature ID	Feature or function	Description	See
Policy enhancements			
SAM-10395	Increasing the bandwidth limit for multicast channels in MCACs	The multicast channel bandwidth in MCAC has been increased to 10 Gbps.	*5620 SAM Parameter Guide*
SAM-11646	Route download policy	The route download policy provides a mechanism to download customer-assigned subnets from a RADIUS server to an NE.	Chapter 49 Procedures 49-7 and 49-9
SAM-12832	Override egress FC for ingress QoS policies	The 5620 SAM now supports explicitly configuring the egress FC in a SAP ingress QoS policy.	Procedure 43-1 *5620 SAM Parameter Guide*
SAM-12866	Auto-generation of filter prefix lists (CPM IPv4/IPv6 apply-path BGP base routing instance, wildcard-only	The 5620 SAM now supports the auto-generation of IP prefix lists for both IPv4 and IPv6. The auto-generated prefix list can be used in CPM filters.	Procedure 44-5
SAM-12887	BGP policy framework: sub-policies	In routing policy statements, you can include sub-policy calls to enable the grouping of match criteria over multiple policy entries for more complex match conditions.	Procedure 22-15
SAM-12936	RFE 135082: M-CAC for (S, G) in VRF; i.e. CAC on # replications per SAP	The Maximum Number of Group Sources Per Group parameter has been added to specify how many SAP group source addresses are allowed per group address.	Procedures 70-12, 68-29, 68-32, 68-49, 68-70, 71-52, 71-55, and 23-48
SAM-13044	Shared RADIUS filter terms	Shared filter entries from RADIUS allow the use of RADIUS parameters to enhance a local IP or IPv6 filter list with dynamic entries which are shared between multiple subscriber hosts. Support for Host Shared Start Entry and Host Shared Count configuration on ACL IPv6 filter policy and ACL IPv6 filter policy.	Procedures 44-2 and 44-3
SAM-13064	HTTP redirection for IPv6 filter policies	The 5620 SAM supports creating IPv6 filter entries that use an HTTP redirect action.	Procedure 44-3
SAM-13067	Flexible IPv6 PD Prefix length	A delegated IPv6 prefix length option has been added to the address pools for local DHCP servers in base routing and VPRN routing instances, as well as to PPP and DHCP hosts for subscriber management. A variable-length option (0) has also been added to the delegated IPv6 prefix length option under subscriber interfaces.	Procedure 71-59 Procedure 22-3 Procedure 65-5
SAM-13076	LAC parameter configuration at site level	You can configure LAC parameters at the L2TP site level, and the parameters can be inherited by child L2TP tunnel group profiles and L2TP tunnel profiles.	Chapter 23 Procedure 23-34
SAM-13745	Policy enhancement: Progress on release	The global policy release and distribution mechanism has been modified. When a global policy is altered and the configuration mode changes from Draft to Released, the change will no longer be automatically released to all local definitions. A release window now opens instead and allows the operator to modify the distribution list. The existence of a previous local definition on any particular NE is also indicated in this window.	Procedure 42-1 Procedure 42-4
SAM-14171	VRRP host unreachable event ICMP packet size	The 5620 SAM supports using the Padding Size parameter to adjust the size of ICMP packets sent due to a VRRP host unreachable event.	Procedure 47-1

(15 of 21)

Feature ID	Feature or function	Description	See
SAM-14180	Port fragmentation support for IPv6 packets in ACL policies	Fragmentation support has been added for IPv6 ACL filter policies for FP2- and FP3-based IOMs/IMMs/X-MASs and C-XMAs on 7750 SR and 7750c12 platforms.	Procedure 44-3 *5620 SAM System Administrator Guide* *5620 SAM Parameter Guide*
SAM-14199	Support for multiple community names in policy statement entries	Two enhancements were made to policy entry usage related to "community". 1:Adding a community list expression to the "From community". 2. The ability to specify multiple community-list names in the action part of a policy entry.	Procedure 22-15
SAM-15087 SAM-15996 SAM-16003 SAM-16014 SAM-16018	Access Egress Queue-Group Instances: Creation, sharing, redirection, and overrides	IOM3/IMM support for Access Egress Queue Group Instance creation, sharing, redirection (from a FC policer to a SAP egress port queue group), and overrides has been added. This feature applies to Ethernet SAPs on VLL Epipe, VPLS, IES, or VPRN services.	Procedure 16-8 Procedure 43-3 Procedure 67-27 Procedure 68-25 Procedure 70-21 Procedure 71-25
SAM-15955	IPv6 prefix list support: IPv6 prefix-list	The 5620 SAM now supports the concept of matching source and destination IP prefix lists for ACL IP filters and CPM filters. This works in conjunction with feature SAM-12866.	Procedure 44-2 Procedure 44-3 Procedure 44-5 *5620 SAM System Administrator Guide*
SAM-16159	RFE 140655: plcy: as path group regular expressions	This feature provides the ability to combine several AS path regular expressions into one construct (an AS Path Group) for matching in a single route policy entry.	Procedure 22-15 Procedure 22-20
SAM-16160 SAM-16167	Access Egress HSMDA Queue-Groups	The ability to allow redirection of FCs belonging to multiple SAPs on egress to a shared set of queues for Ethernet HSMDAv2 MDAs has been added.	Procedure 16-8 Procedure 43-24 *5620 SAM Statistics Management Guide*
SAM-16922	RFE 128937: New combined-network-ingr-egr Accounting Policy	A new record type (Complete Network Ingress Egress) has been added to accounting policies. The new single record combines information available in network ingress packets, network egress packets, network ingress octets, and network egress octets records.	Section 77.5 Procedure 43-24
SAM-17968	VRRP policy MC-IPsec Non Forwarding events	The 5620 SAM supports creating MC-IPSec Non Forwarding events on VRRP policies to track the MEP state of a DUT.	Procedure 47-1
SAM-19006	DCR 646149: Global Policy Check	Global ACL policies are now checked before distribution to the network. If the policy is empty, a warning is issued due to the potential impact of distributing such a policy to the network.	Procedure 44-1 Procedure 44-2 Procedure 44-3
SAM-19121	DCR 590994: Routing Policy From criteria protocol not listed	The Managed option has been added to the From criteria of a routing policy.	Procedure 22-15
SAM-19177	DCR 629502: Request to add a QoS Description field	A Description field has been added to the QoS policy added under the QoS tab on the SAP form.	Procedure 43-1 Procedure 43-3 Procedure 43-24
SAM-19369	RADIUS authentication request and accounting request scripts	The RADIUS server policy supports separate RADIUS accounting request script and authentication request script configuration. The new configuration replaces the old RADIUS request script configuration.	Procedure 49-4

(16 of 21)

Feature ID	Feature or function	Description	See
SAM-19785	RFE 128459: Port scheduler max-rate and scheduler rate range changes for FP3 IOMs	The port scheduler rate maximum range value has been increased to 400 G. The scheduler rate maximum range value has been increased to 800 G.	*5620 SAM Parameter Guide*
Service management enhancements			
SAM-288	L2-aware NAT on dual stack subscriber	Support for IPv6 host coexistent with an IPv4 L2-aware host under the same subscriber. This, in turn, requires PPPoE anti-spoof configuration on IES and VPRN group interfaces.	Procedures 70-12 and 71-60
SAM-11604	Base routing interfaces respond to traffic when GRT leaking enabled	Base routing instance interfaces reply to traffic originated from a VPRN that is leaked to GRT. GRT leaking is enhanced to enable system interfaces to respond to leaked routes. You can enable GRT self-generated traffic. The VPRN network can access global interfaces on the PE.	Procedure 71-9
SAM-11881	Tethering detection	You can enable tethering detection for an AA group or partition on a Release 5.0 or later 7750 MG.	Procedure 14-2
SAM-12970	Tunnel administrative groups	In releases prior to release 11.0, 5620 SAM steering parameters are applied on tunnel selection profiles. In the 5620 SAM, Release 11.0 and later, steering parameters are enhanced and renamed as tunnel administrative groups, and provide the additional support of SDP selection. Tunnel administrative groups allow services that use a PW template to automatically include or exclude specific provisioned SDPs. You can apply tunnel administrative groups to: • service tunnels • tunnel selection profiles • service PW templates • BGP or BGP AD VPLSs	Chapters 27 and 79
SAM-12990	IPv4 multicast for routed VPLS	The 5620 SAM supports IPv4 multicast over a routed VPLS service.	Chapter 68
SAM-12998	mLDP P2MP LSP support for provider tunnels	The 5620 SAM supports setting the Type of the P2MP LSP of a provider tunnel to mLDP.	Procedure 68-12
SAM-13000	Routed I-VPLS support	The 5620 SAM supports binding an I-VPLS to an L3 access interface, and using I-VPLS services and I-sites to create routed VPLS connectors for composite services.	Section 68.1 Chapter 74 Procedures 68-65, 70-19 and 71-30
SAM-13002	Ignore failed SAP on an Epipe service	The 5620 SAM supports configuring an Epipe service to remain in an Up state when selected SAPs fail by enabling the Hold Service Up On SAP Failure parameter on the SAP.	Procedure 67-27
SAM-13020	VPRN support of BGP confederations	You can configure BGP confederation autonomous systems on VPRN routing instances.	Procedure 71-8
SAM-13026	Open DHCP model	IPv6 configuration enhancements on local user database DHCP and PPP hosts.	Procedure 65-5
SAM-13038	Local user database MSAP defaults for IPoEv6	You can specify a local user database for DHCPv6-triggered host authentication on a capture SAP.	Procedure 65-28

(17 of 21)

Feature ID	Feature or function	Description	See
SAM-13042	Ignore magic number check	You can configure the 5620 SAM to ignore magic number checks in an LCP Echo-Request or Echo-Reply message. The LCP Ignore Magic Number parameter can be configured on an L2TP tunnel group profile, L2TP tunnel profile, and on a PPP policy.	Procedure 23-34
SAM-13048	DHCP relay proxy	Support for Relay Unicast Message configuration on L3 access interfaces and group interfaces on IES or VPRN services.	Procedures 70-1, 70-12, 71-22, and 71-60
SAM-13050	RADIUS-triggered dynamic service creation	The 5620 SAM supports configuring 7750 SR and 7450 ESS nodes to create services using information contained in RADIUS CoA messages instead of manual input.	Chapter 75
SAM-13054	Subscriber services information retrieval	You can retrieve read-only subscriber service (RaBaPol) information from a subscriber host.	Chapter 65 Procedure 65-13
SAM-13056	Default primary and secondary IPv6 DNS server address on IES and VPRN subscriber interface	Support for Default Primary IPv6 DNS Server Address and Default Secondary IPv6 DNS Server Address configuration on IES and VPRN subscriber interface.	Procedures 70-10 and 71-59
SAM-13060	ANCP enhancements	Support for Persistency Database and Idle Filter configuration on GSMP group on VPRN and VPLS service site. Ability to retrieve ANCP subscriber line information from a subscriber instance, as well as from an ANCP static map on an L2 access interface, L3 access interface, aggregation scheduler, or SAP. New RADIUS parameter (Access Loop Option) on RADIUS accounting policy.	Procedures 68-18, 71-13, and 65-15
SAM-13070	Local user database subnet draining with primary/secondary address pools	Local DHCP servers, and local DHCP and PPP hosts, support the configuration of a second host address pool to facilitate subnet draining. You can enable subnet draining on a local DHCP server in a base or VPRN routing instance.	Procedure 22-1, for local DHCP server configuration steps Procedure 65-5, for local user database configuration steps Procedure 65-6, for subnet draining configuration steps
SAM-13072	LLID pre-authentication	NAS Port Bit Specification configuration on subscriber authentication policy. Configuration of a pre-authentication policy on a local user database.	Section 49.1 Procedure 65-5 *5620 SAM System Administrator Guide*
SAM-13074	Local user database VLAN range support	You can configure a VLAN range as a DHCP or PPP local user database host identification criterion.	Procedure 65-5
SAM-13082	Ingress MAC filter on Capture SAP	The 5620 SAM supports configuring a MAC ingress filter on a capture SAP. The Type parameter of the MAC filter must be set to VID.	Procedure 65-28
SAM-13084	Unnumbered model for IPv4 and IPv6 IPoE	Support for Allow Unmatched Subnets configuration on VPRN and IES subscriber interfaces.	Procedures 70-10 and 71-59
SAM-13100	Data-triggered UE authentication	Support for data-triggered UE creation and authentication on WLAN-GWs. Authentication is via an authentication policy, with a configurable authentication hold time.	Procedure 70-13

(18 of 21)

Feature ID	Feature or function	Description	See
SAM-13112	RTSP header and URI classification	RTSP headers are selectable as application filter expression criteria in an AA group policy for a Release 11.0 or later 7450 ESS or 7750 SR, a nd for a Release 4.0 R5 or later 7750 MG.	Procedure 76-1
SAM-13116	RADIUS Export of application group, XML export of charging group	During AA group policy configuration, you can specify an application or application group identifier that is included in accounting records, and a charging group identifier that is available to OSS clients.	Procedure 76-1
SAM-13124	AARP enhancement	On an AARP instance, you can specify the master selection algorithm.	Procedure 76-2
SAM-13130	Focused cflowd	You can configure cflowd samplers to measure RTP and comprehensive performance.	Procedure 14-4
SAM-13132	Time of day policer rate adjustment	You can configure a time-of-day override for an AA policer.	Procedure 76-3
SAM-14200	Filter under NAT SAP	You can specify an ACL IP filter for upstream NAT traffic on a base or VPRN routing instance.	Procedure 24-3
SAM-14202	Protocol number added to AQP match criteria	You can specify a transport-layer protocol as an AQP match criterion.	Procedure 76-5
SAM-14204	HTTP redirect for added as AQP action	You can specify an HTTP redirect as an AQP action.	Procedure 76-5
SAM-14267	Residential summarization groups	AA partitions and unpartitioned AA groups support the configuration of residential DCP groups that specify how to summarize the data that is forwarded to the 5670 RAM. The data can be summarized by subscriber or content-server IP address to help identify regional traffic patterns of interest.	Chapter 76 Procedure 14-2
SAM-14973	5670 RAM: IP detail configuration	Services that support AA can be configured to report the IP addresses of the top users of specific applications and application groups to the 5670 RAM.	Chapter 76 for general information, and the following: Chapter 70, for IES Chapter 67, for VLL Chapter 68, for VPLS Chapter 71, for VPRN
SAM-15694	Strict no ECMP mode for uPRF	You can configure an interface that is not on an ECMP route to drop any ECMP packets by setting the uPRF mode to Strict No ECMP.	Procedure 22-10
SAM-16639	7750 SR firewall	AA session filters are now configurable for a Release 11.0 or later 7750 SR.	Procedure 76-24
SAM-21153	Multiple PPP sessions using one MAC address	In a PPP policy, you can specify how many PPP sessions to allow for one host MAC address. You can also specify whether to allow DHCP sessions on the same circuit as the PPP sessions.	Procedure 54-4
SAM-22113	Application filter entry renumbering	To accommodate the insertion of new application filter entries, you can renumber multiple existing filter entries in one operation.	Chapter 76 Procedure 76-4
OAM and service testing enhancements			

(19 of 21)

Feature ID	Feature or function	Description	See
SAM-1215 SAM-10424 SAM-10443 SAM-13231 SAM-13724	OAM Test Result Structures	The OAM test results database has been re-structured to increase the performance and storage capacity of test and test suite results.	Procedure 32-44 Procedure 77-5 Procedure 77-8 Procedure 77-11 Procedure 77-12 Procedure 77-13
SAM-12870	Twamp Server support extension	Twamp Server support extended to include IPv6	Procedure 13-11
SAM-12872	Ethernet CFM - Symmetric QoS/CoS behavior	A property has been added to allow specifying the Linktrace Response (LTR) value for a MIP.	Procedure 78-1 *5620 SAM Parameter Guide*
SAM-12876	Ethernet CFM Primary VLAN support	The Primary VLAN feature allows an operator to set a VLAN identifier to perform additional ETH-CFM extraction checking. Primary VLAN enabled MEPs (on VPLS and Epipe services) will only perform the additional extraction routines for MEPs configured under the same SAP and that have an enabled Primary VLAN.	Section 78.1 Procedure 78-1 Procedure 68-37 Procedure 67-27
SAM-12880	802.3ah enhancement - EFM passive status	The Ignore EFM State property has been added to allow specifying the effect of a port's EFM-OAS status on the operational state of that port	Procedure 32-42 *5620 SAM Parameter Guide*
SAM-14174	Configurable ping size of up to 1500 bytes for static cpe-check	A configuration option has been added for static routes (IPv4/IPv6) with CPE-check enabled to allow setting the packet length used for ICMP ping test messages.	Procedure 22-13 *5620 SAM Parameter Guide*
SAM-14207	Facility MEP enhancement	ETH-CFM Port & LAG Facility MEPs now support Null encaps in Access and Network modes.	Procedure 78-1
SAM-14209 SAM-15560	Extended VCCV-Ping and VCCV-Trace support for VPLS Test Suite	The 5620 SAM now support the selection of Spoke-SDPs within a VPLS for VCCV-Ping and VCCV-Trace tests	Procedure 32-23 Procedure 32-24 Procedure 77-1
SAM-14211	Align spoke-interface behavior of vprn-ping and vprn-trace with that of a SAP	Spoke interface behavior has been modified to match that of a VPRN SAP. In this way, packets are never forwarded over the spoke interface, but a reply will be made if the prefix is reachable via the spoke interface. Otherwise, the packet is dropped in CPM.	*5620 SAM Parameter Guide*
SAM-15563	VPLS map changes for VCCV-Ping and Trace for PW	The VPLS/MVPLS service map now supports the creation of the VCCV-Ping and VCCV-Trace tests.	Chapter 32
SAM-20357	RFE 130107:VCCV-Ping Test Suite generation for H-VPLS & Service Connector	The OAM VCCV-Ping test has been added to the Test Suite test generation for H-VPLS & Service Connectors	Procedure 32-23 Procedure 77-1
5620 SAM documentation enhancements			
—	Creation of a new *5620 SAM System Administrator Guide*	Consolidates many of the tasks performed by a user with a 5620 SAM admin role into a separate guide. The primary areas covered include: • 5620 SAM and UNIX security management • advanced configuration • routine maintenance The former *5620 SAM Maintenance Guide* has been incorporated into this new guide.	*5620 SAM System Administrator Guide*

(20 of 21)

Feature ID	Feature or function	Description	See
—	Creation of a new *5620 SAM LTE OSS Interface Developer Guide*	Provides information about developing LTE OSS applications, including information about the 3GPP OSS interface components and architecture, understanding the 5620 SAM-O schema in the context of LTE, compliance with 3GPP standards, and typical operational scenarios. The former *5620 SAM 3GPP OSS Interface Developer Guide* and *5620 SAM 3GPP OSS Interface Compliance Statements* documents have been incorporated into this new guide.	*5620 SAM LTE OSS Interface Developer Guide*
—	Parameter search tool added to on-line user documentation	A new Parameter search tool is available in the on-line user documentation. You can search for details about a particular parameter using either its displayed name on the GUI or its OSS (XML) name. You can also use the tool to display all parameters on a form.	Section 3.1 Procedure 3-14

(21 of 21)

2 — 5620 SAM system overview

2.1 5620 SAM system overview *2-2*

2.2 About this guide *2-3*

2.1 5620 SAM system overview

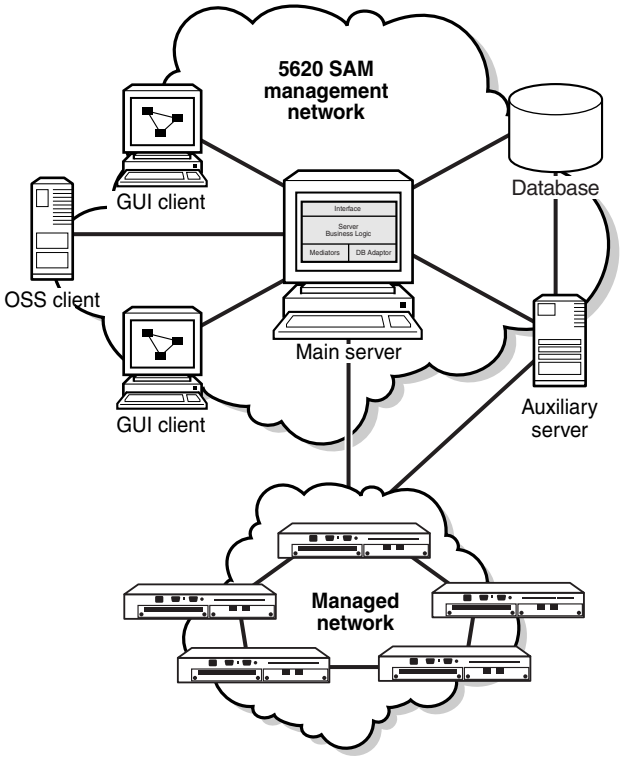
The Alcatel-Lucent 5620 Service Aware Manager, or 5620 SAM, enables end-to-end network and service management of Alcatel-Lucent NEs, and limited management of third-party NEs. Third-party NEs are referred to as generic NEs, or GNEs. The 5620 SAM enables you to perform tasks that include the following:

- Provision a network with fast and easy configuration and multi-vendor scripting workflows that reduce risk of error and shorten network deployment time.
- Accelerate setup for integrated IP/optical performance and SLA monitoring with service-aware diagnostics that validate end-to-end services and IP/optical paths.
- Prevent service degradation through end-to-end power control, monitoring, tracing. and fault localization.
- Correlate faults to identify whether the problem resides in the IP or optical layer, and the root cause. This function simplifies troubleshooting and isolates problems before services are affected.

5620 SAM system architecture

A basic 5620 SAM system has client, server, and database components that are deployed in a standalone or redundant configuration. Figure 2-1 shows a simple 5620 SAM management network, which contains the 5620 SAM components, and a managed network of NEs.

Figure 2-1 Standalone 5620 SAM system



A 5620 SAM operator performs network management or system administration tasks using a GUI or OSS client that connects to a main server. The main server sends and receives NE management traffic, and directs optional auxiliary servers to perform tasks such as NE statistics collection. Main and auxiliary servers store information in the same 5620 SAM database.

See the *5620 SAM System Architecture Guide* for detailed system design information.

Supported network management modules

The 5620 SAM provides network management functionality using the following modules:

- SAM-A—OAM tools, service assurance functions, fault correlation using alarms, topology views, and statistics management
- SAM-E—device mediation, equipment navigation and management, security, CLI access, backup and restore, alarm management, real-time equipment statistics, and inventory and reporting
- SAM-O—OSSI package that includes an HTTP SOAP interface for general network management and configuration, a subscription-based JMS interface for event monitoring, and 3GPP-compliant CORBA and TAO interfaces for LTE network management
- SAM-P—service provisioning, templates, and management of customers, subscribers, tunnels, paths, and policies
- Mobile Services Package—LTE-specific package for LTE NE discovery and LTE network management
- Supervision module—a web-based application that provides alarm monitoring based on user-defined views and groups

2.2 About this guide

The *5620 SAM User Guide* provides information about using the 5620 SAM to manage service-aware IP/MPLS networks, including GUI operations, device and network management, and policy and service management.

This guide contains the following volumes:

- Getting started—contains general 5620 SAM information including the following:
  - a system overview
  - feature lists by release
  - basic GUI operation instructions
  - GUI map management
- Device management—contains information about device functions that are not directly related to networking, including the following:
  - device support
  - preparing devices for 5620 SAM management
  - 5620 SAM device and equipment management functions

- Network management—contains information about network functions including the following:
  - general routing and forwarding
  - protocol-specific routing and forwarding
  - traffic management using MPLS and service tunnels
  - fault management
  - OAM diagnostic tests
  - NE redundancy
- Policy management—contains information about configuring and applying 5620 SAM policies that define rules for NE, network, or 5620 SAM operation
- Service management—contains information about managing customer services, including the following:
  - service creation and configuration
  - customer and subscriber management
  - service verification, troubleshooting, and root-cause analysis
  - scheduling of routine, service-related operations

3 — 5620 SAM GUI overview

3.1 5620 SAM GUI overview *3-2*

3.2 Using search functions *3-16*

3.3 Workflow to use the 5620 SAM GUI *3-21*

3.4 5620 SAM GUI opening and closing procedures *3-21*

3.5 Basic 5620 SAM GUI operation procedures *3-31*

3.6 5620 SAM GUI user preferences configuration procedures *3-40*

3.7 5620 SAM GUI search procedures *3-45*

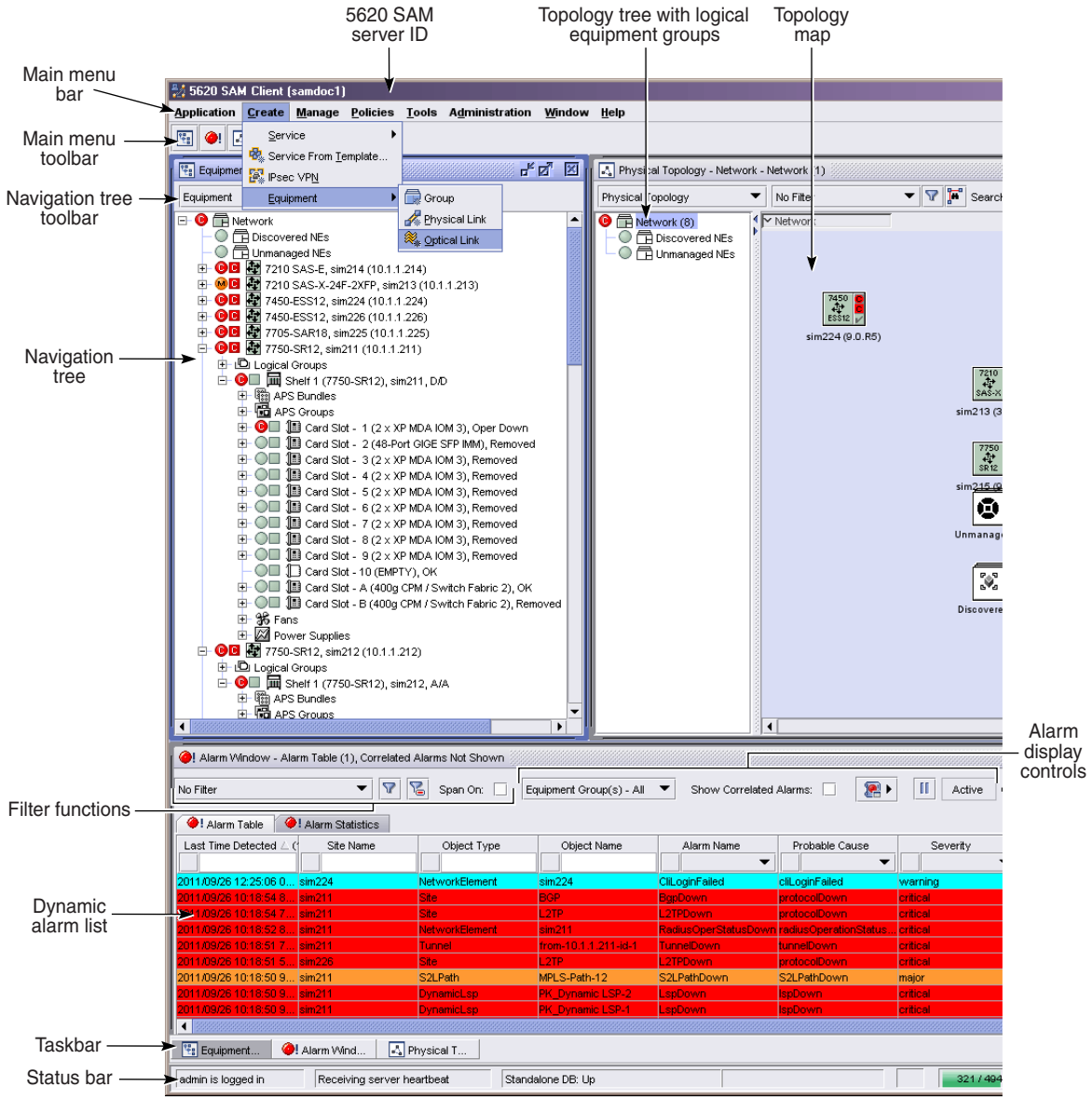
3.1 5620 SAM GUI overview

The 5620 SAM GUI on a 5620 SAM client station allows an NOC operator to perform device, network, policy and service management functions. Multiple 5620 SAM GUI clients can connect to a 5620 SAM server.

This chapter describes general GUI operations such as starting and stopping the GUI, configuring GUI user preferences, creating, managing, and customizing workspace elements, basic GUI operations, and performing searches on the GUI.

The main GUI workspace elements are shown in Figure 3-1.The three main windows, which open by default, display the navigation tree, Alarm Window, and topology map.

Figure 3-1 Main 5620 SAM GUI elements



20995

Custom workspaces

The 5620 SAM supports custom workspaces. You can configure menus, toolbars, navigation tree labels, map icon labels, and window displays to suit your operational requirements. You can save and select private and public workspaces, and update saved workspaces after a 5620 SAM upgrade. You must have the required scope of command permissions to customize workspaces. Permissions for workspaces are set by a system administrator. See "5620 SAM custom workspaces" for more information.

Shortcut keys

Menu items can be accessed using shortcut keys. To access menu items using the shortcut keys, simultaneously press ALT-*key* where *key* is the underlined letter of a top level of the main menu. For example, ALT-P displays the Policies menu. Pressing a key that corresponds to the underlined letter of a displayed menu item opens that item.

Windows and forms

The 5620 SAM GUI displays windows and forms. The main GUI workspace elements, which are displayed in windows, are the navigation tree, Alarm Window, and topology map. Forms are displayed in response to menu options, icons, or shortcut keys, and are typically used to configure device and 5620 SAM parameters. Forms are also used to display the status of objects, or to perform FCAPS operations. Forms allow searches, display lists and provide options. See "Forms" in section 3.1 for more information.

Multi-edit property forms

The 5620 SAM GUI allows users to configure multi-value fields that are common to all property forms. Multi-edit values include text fields, number fields, mirrored property fields, and combo boxes. Changes made are propagated to all objects that are multi selected. The following apply:

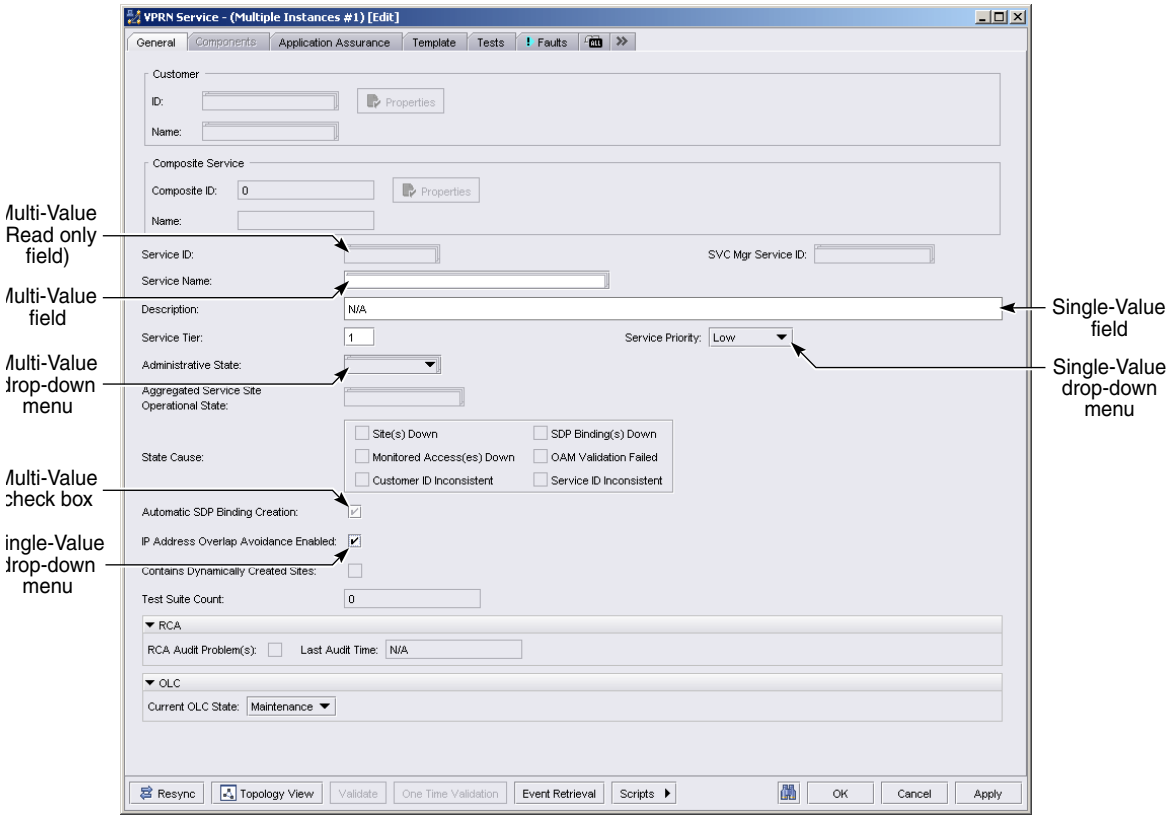
- If a field is read-only it is dimmed.
- Property values that are different across property forms are displayed as a multi-value field and can be edited, if they are not read-only.
- Property values that are the same across property forms are displayed as a single value field.
- If a cursor is displayed in a multi-value field and no value is entered, the field still displays a multi-value when the cursor is moved to another field.
- If a value is entered, the field is no longer multi-value, and the new value is applied to all instances edited when a user applies the changes.
- If a previously populated value is set to blank, and a user applies the change a warning message is displayed. The warning message contains the field names with the corresponding tab names.



Note — The OK and Apply buttons are disabled if a mandatory field is left blank, even if other values have been changed on the form. When the mandatory field is updated, the OK and Apply buttons are enabled.

Example 1: A user edits two objects, one with a description field entered, and the other description field is blank. The multi-value description field on the Multiple Instances (Edit) form is displayed. When the user sets the field value to blank in the Multiple Instances (Edit) form, both the property forms will have a blank description. When the user applies the changes a warning message is displayed.

Figure 3-2 Multi-value property form



23740

5620 SAM clipboard

You can use the 5620 SAM clipboard to save and copy property form identifier links. A property form identifier link is a unique internal address that the 5620 SAM assigns to a form or window. Multiple property form identifier links can be saved to the 5620 SAM clipboard at the same time, and then used for navigating to the forms that they identify. See Procedures 3-15 and 3-16.

Note — The Copy Property Form Identifier is applicable only to property, alarms and statistic forms.

Floating windows

The 5620 SAM GUI has floating windows that you can move, size, hide, and move to the foreground to provide the required workspace to perform a task. By default, the navigation tree window appears on the left side of the GUI, the physical topology map window on the right, and the Alarm Window on the bottom.

If you need to move a window or form to the foreground, click on a taskbar button, choose a window menu item, or press the shortcut keys. If you need to open a closed window or form, select a toolbar icon, choose an application menu item, or press the shortcut keys.

User preferences

You can use the user preferences form to customize the localized client settings for a number of GUI, statistics plotter, script management, and workspace settings to meet your specific operational requirements. Table 3-5 lists the location of user preference information in the 5620 SAM customer documentation suite. You can access the User Preferences form from the Application menu. You can configure user preferences for the following settings:

- Configuration forms, default time zones, span of control, topology windows, alarm windows, to access test objects, to initiate bulk change operation, to display the number of objects on a list form.
- Statistics plotter
- Script management
- Workspace customization

See section 3.6 for more information.

System preferences

You can use system preferences to customize or change the default value for a number of 5620 SAM global settings and functions to meet your specific operational requirements. You need a user account with the Administrator scope of command role to configure system preferences. You can configure system preferences for the following settings and functions:

- General preferences
- Services
- TCA alarms
- Statistics
- STM
- User activity
- OLC state and scheduling
- Policies
- Custom NE properties



Caution — Changing a system preference parameter value may adversely affect the 5620 SAM service or function. Do not change the parameter value from the default without contacting Alcatel-Lucent technical support.

You can access the System Preferences form from the Administration menu. See the system preferences configuration information in the *5620 SAM System Administrator Guide*.

External windows

A window or form in the GUI can be moved out of the main workspace and managed as an external window; for example, on a second monitor. For more information about managing external windows, see Procedure 3-10.

External windows are managed by the operating system (and not the 5620 SAM). They maintain the window icon that is used in the GUI and are placed in a group of open 5620 SAM windows on the operating system taskbar. Any windows or forms that are opened from an external window appear as separate external windows. The 5620 SAM GUI taskbar does not display external windows, but they can be viewed and moved to the foreground using the Window menu. The Window menu also contains options to Close All Internal Windows or Close All External SAM Windows.



Note — An external window or form cannot be moved back to the 5620 SAM GUI. You must close the external window and re-open the window in the GUI.

Navigation tree

The navigation tree lists the managed equipment, services, and protocols that are configured on the NE. The navigation tree includes a view selector located on the navigation tree toolbar. The view selector is a drop-down menu that lists the physical and logical network views that are available.

The navigation tree is accessible from the main workspace, configuration forms, and maps.

See chapter 5 for more information about the navigation tree.

Contextual menus

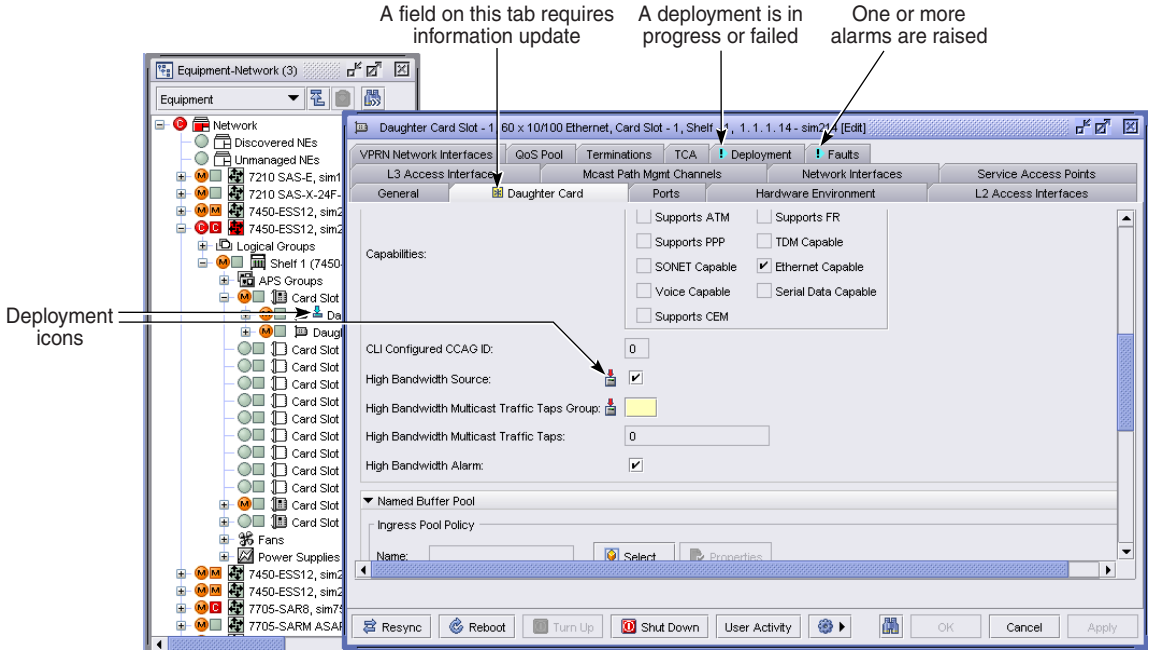
Contextual menus allow you to create, configure, and manage specific parameters for the object and child objects from the navigation tree or from maps. You access the contextual menus by right-clicking on the navigation tree object or on the map object.

See chapter 5 for more information about contextual menus.

Indicators and icons

Indicators and icons inform you of activity that is in progress or requires attention, and can appear and disappear depending on the activity that is occurring in the 5620 SAM, as shown in Figure 3-3.

Figure 3-3 Indicators and icons



22870

For instance, a warning indicator appears on the Deployment tab when a configuration change is not fully deployed to an NE. A warning indicator appears on the Faults tab when the 5620 SAM has raised alarms against the object or a related object. An asterisk appears on a tab or panel title bar to indicate that a field contains incorrect data, or that a mandatory field requires data.

A deployment icon appears beside parameters on an object properties form for which a deployment is in progress or has failed, beside affected navigation tree objects, on info tables in map views, and in list forms.

An asterisk on a tab or panel title bar indicates that a field contains incorrect data, or that a mandatory field requires data.

See chapters 12 and 31, and "Collapsible panels" in this chapter for more information.

Additional Text Find icon

The Additional Text Find icon is available on object property forms. See Procedure 31-5 for more information. You can configure an additional text policy to display specific information about an alarmed object in the additional text column of the dynamic alarm list and on the Alarm Info form.

Task manager

The Task Manager allows 5620 SAM administrators and support personnel to monitor progress of operational tasks. To monitor the 5620 SAM Task Manager, see Procedure 3-23.

The Task Manager monitors the following operations:

- all write operations that are performed from the 5620 SAM GUI; for example, when you click on the Apply or OK buttons
- all write operations that are performed using the OSSI
- some read operations; for example, when you click on the Resync or Collect All buttons

Only 5620 SAM administrators can change the Task Manager default settings. See "To change the 5620 SAM Task Manager default settings" in the *5620 SAM System Administrator Guide*.

Text message

Users can send broadcast messages to some or all active GUI users logged into the 5620 SAM. This is useful for sending maintenance and similar notifications to active users.

See Procedure 3-11 and "To send a broadcast message to 5620 SAM GUI users" in the *5620 SAM System Administrator Guide* for more information.

Maps

Each map displays network objects and information, and provides contextual menus to open forms that display additional information. In the context of a 5620 SAM map, a link object, such as a physical link or service tunnel, is called an edge. An object other than a link between objects, such as an NE or a topology group, is called a vertex.

See chapter 6 for more information on maps.

Alarm Window

The Alarm Window allows you to view and manage incoming alarms from network components which are displayed in the dynamic alarm list and are associated with objects that represent the affected network components.

See chapter 31 for more information on the Alarm Window.

Forms

5620 SAM forms are used to do the following:

- configure device and 5620 SAM parameters
- display the status of an object
- perform FCAPS operations

A form can be displayed anywhere in the GUI. A newly opened form is displayed in the foreground. You can do the following:

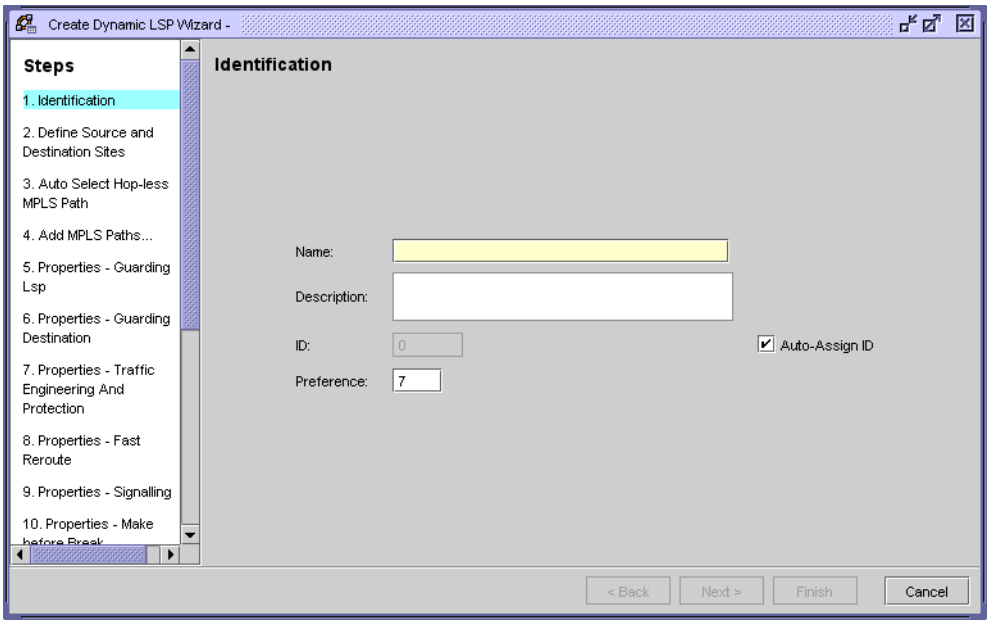
- organize forms according to operator preference
- compare information on multiple open forms
- navigate quickly to another open form by choosing the form from a list

A form has a title bar that displays object information. The displayed object name is the name specified during object creation. If the object is not named, a default name is used. When a form is minimized, a tool tip displays the title bar information. The Window menu lists the open forms.

Some configuration activities lead the operator through a series of forms, each of which represents a step in the configuration process. Such a form is called a step form. You must click on the Next button to proceed to the next step. Figure 3-4 shows the first step in a step form sequence. When the configuration sequence is complete, you must click on the Finish button to commit the changes. Each step must be performed to complete the configuration activity.

Note — Some steps open a new step form. You must complete the steps in the new form before you can return to the previous form. After you click on the Finish button, the previous form reappears.

Figure 3-4 Step form



More Actions button

Several buttons appear at the bottom of the 5620 SAM configuration forms and on the right panel of list forms, as shown in Figure 3-7, that perform various functions. Buttons that do not fit are available as a menu item when you click on the More Actions button, as shown in Figure 3-6. In addition, some of the buttons may not be visible when you resize a form. The affected buttons become menu items when you click on the More Actions button.

To resize a form, click on the maximize or restore button at the top right corner of the form, or click on a border or corner and drag the border or corner to shrink or enlarge the form.

User Activity button

The User Activity button on an object properties form opens a form that lists the recent 5620 SAM user actions performed on the object. See "User activity logging" in the *5620 SAM System Administrator Guide* for more information.

Custom tab display

Some forms in the 5620 SAM open by default with hidden tabs. You can display selected hidden tabs or all tabs while the form is open by clicking on the tab selector or the Show All Tabs button. See Procedure 3-21.

You can also customize the display of tabs on configuration forms, and save your tab display preferences. For specific forms, you can display, hide, or arrange the sequence of tabs according to your operational requirements. See Procedure 3-20. Custom settings for tabs on configuration forms are saved as user preferences. They are not affected by a change of workspaces.

A system administrator can configure the default behavior for custom tab configuration from the System Preferences form. See the *5620 SAM System Administrator Guide*.

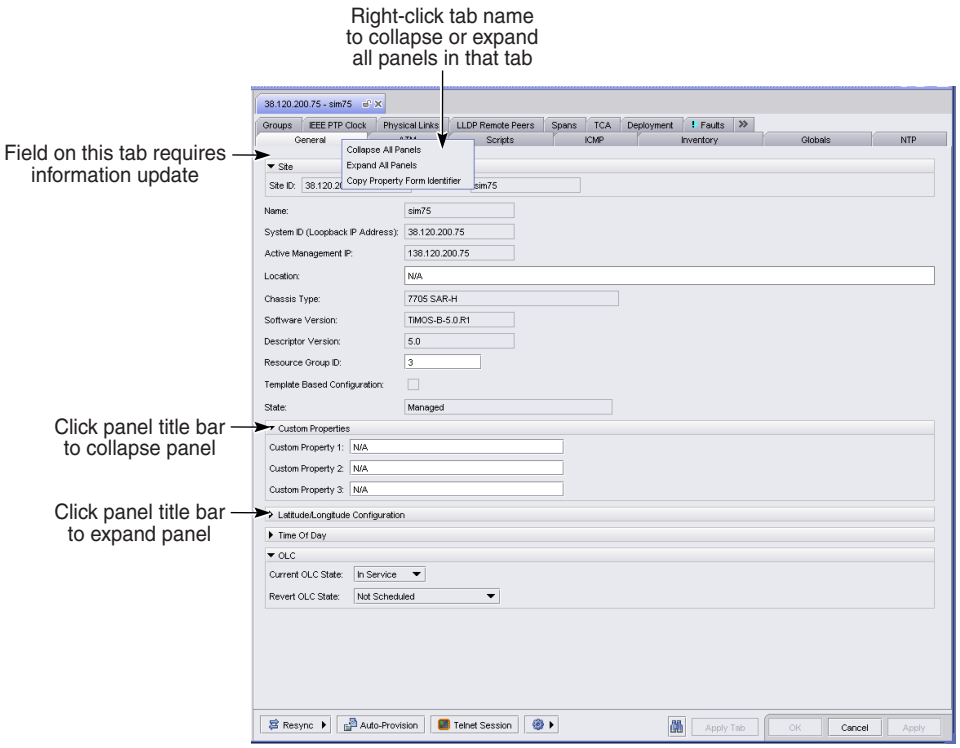
Collapsible panels

The 5620 SAM form panels can be collapsed to hide areas that are not of interest to the specific user or expanded to display all areas in a form.

To collapse or expand a panel, click on the title bar of the panel, as shown in Figure 3-5. You can collapse or expand all of the panels on the tab by right-clicking on the tab title and then choosing the Collapse All Panels or Expand All Panels option.

When a configuration form closes, the current state of the panel is saved for that object type. When a user opens a configuration form, the last saved state of the panel is displayed.

Figure 3-5 Collapsible panels in forms



23726

Navigating service configuration forms

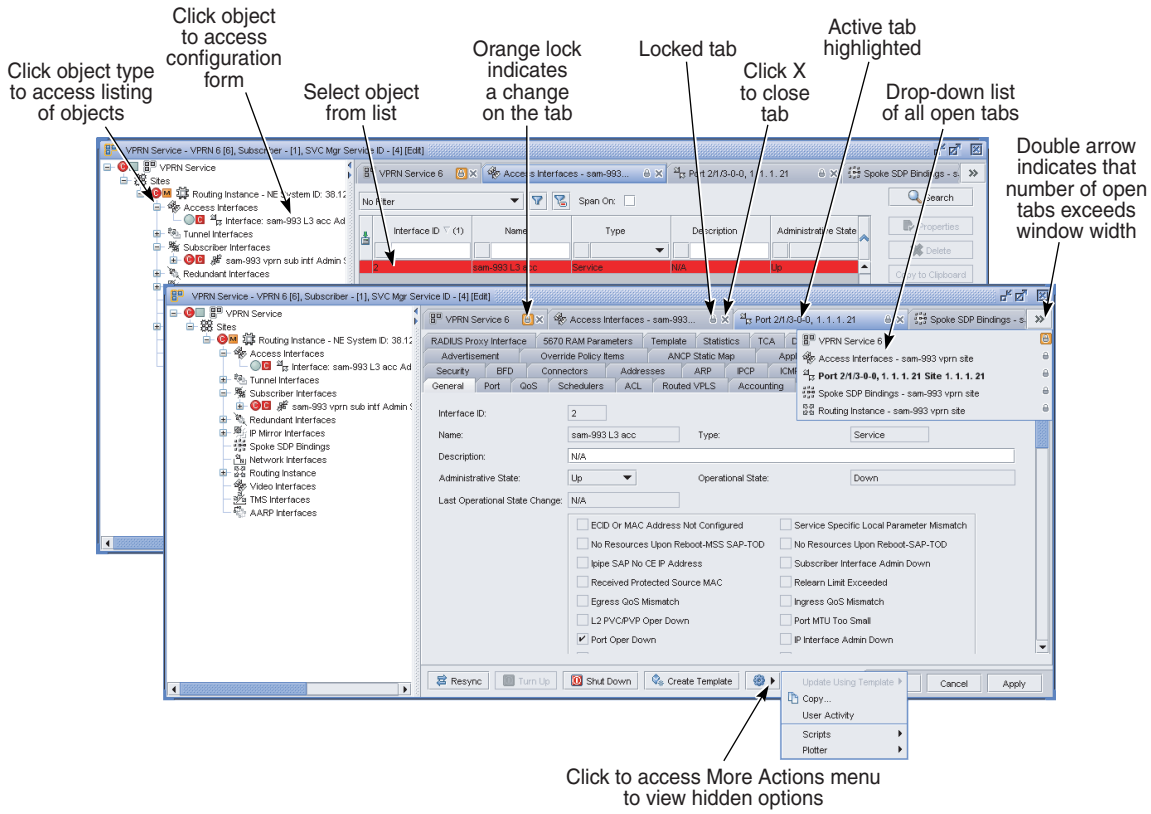
Service configuration forms allow you to create and manage services in the 5620 SAM. You can access service configuration forms from the Create menu or the Manage menu.

When you first access a service configuration form, the form displays a navigation tree on the left and the General tab on the right. The navigation tree lists the objects that are configured for the service. To access the configuration forms for the individual objects from the navigation tree, use one of the following methods:

- Click on the object type to access a filterable list form and choose the object.
- Click on the object in the navigation tree.

Figure 3-6 shows both methods of accessing object configuration forms from the navigation tree.

Figure 3-6 Service configuration form navigation



Navigating network element configuration forms

NE configuration forms allow you to create and manage network devices in the 5620 SAM. You can access NE configuration forms from the following locations:

- 5620 SAM GUI navigation tree. See Procedure 13-2 for more information.
- Manage menu
- Physical topology map
- Service tunnel topology map

When you first access an NE configuration form, the form displays a navigation tree on the left and the General tab on the right. The navigation tree lists the devices that are configured on the NE. To access the configuration forms for the individual devices from the navigation tree, click on the object in the navigation tree.

See chapter 5 for information about navigation tree capabilities.

Displaying multiple configuration forms

When you first access a configuration form, the form is unlocked. If you choose another object from the navigation tree, the unlocked form is replaced by the newly selected object configuration form. To lock the configuration form, click on the open lock icon on the configuration form tab, or right-click on the tab and choose lock from the drop-down menu. When the configuration form is locked, the form remains open until the user closes the form. You can add configuration forms to the workspace by choosing objects from the navigation tree and then locking each form.



Note — Locked forms can only be closed (and not unlocked).

Each form is represented by a tab. If the tabs of the open forms exceed the width of the window, double arrows are displayed. Click on the double arrows to display a drop-down menu of the open configuration forms. You can access the open configuration forms from the drop-down menu or from the tabs. Figure 3-6 shows multiple open service configuration forms and the navigation options.

Object configuration forms can be undocked from the main configuration form window by right-clicking on the component tab title and selecting Undock. The undocked form opens in a new window and the configuration form tab is removed from the main configuration form window. Any changes that are made on the undocked object configuration form are immediately sent to the server.



Note 1 — The root object of the configuration form cannot be undocked, for example the IES service configuration form.

Note 2 — List forms cannot be undocked, for example a listing of access interfaces on a site.

Note 3 — Undocking is not supported on (Create) forms.

Note 4 — Any modified tab cannot be undocked

When the mouse point moves over the object form label, a tool tip displays a descriptive label for the form.

Modified configuration forms

If a configuration form is modified, the form changes to locked and the lock icon appears in orange to indicate that a modification occurred.

For service configuration forms, if an object is added to the service configuration, the new object appears in the navigation tree and the configuration form is displayed with the orange lock icon. The icon remains orange until the modifications are saved or discarded.

For equipment configuration forms, if an object is added from the navigation tree, the change will be made immediately. However, if a change, such as adding or removing an object, is made to an equipment configuration form, the change will be reflected on the form immediately, but it will not be reflected on the navigation tree until the Apply Tab, OK, or Apply button has been pressed.



Note — For the NE and composite service configuration forms, changes implemented by pressing the Apply tab apply only to the current object-level tab. Changes implemented by pressing the OK, Apply, or Cancel buttons apply to the entire form.

If you attempt to close a modified configuration form that contains unsaved changes, a message prompts you to specify whether to discard the changes or return to the display. If you attempt to close a modified configuration form that has related forms with unsaved modifications, the message lists the forms that have unsaved changes.

Parameter Search Tool

The Parameter Search Tool is part of the online user documentation that is available under Help→User Documentation in the 5620 SAM client main menu. The tool allows you to view information about parameters and configuration forms in the 5620 SAM. You can select a form name from a list of configuration forms, or you can search using one of three criteria:

- Parameter GUI display name
- Parameter XML name
- Form GUI name

Search results contain information about forms and parameters, including applicable devices, restrictions, the defaults and ranges of parameters, and other information. The information is displayed in HTML format in a web browser. Dynamic links allow you to navigate the tool to access more information, such as parameter options (also called enumerations).

The Parameter Search Tool does not include information about some types of forms or parameters that are specific to the 5620 SAM, such as:

- User preferences
- System preferences
- OLC state
- Faults or Deployment tabs

For parameters not included in the Parameter Search Tool, information is available in the *5620 SAM Parameter Guide*.

See Procedure 3-14 for information about how to use the Parameter Search Tool.

Localized language support

The 5620 SAM GUI supports localized language display. Localized language display, also known as internationalization, displays 5620 SAM GUI text in a specified language. The localized language setting applies to most 5620 SAM GUI objects, except system components and database objects. Contact Alcatel-Lucent support for more information about localized language support.

Note 1 — The 5620 SAM supports localized language settings using predefined strings, and does not translate data to different languages.

Note 2 — The 5620 SAM-O does not support language localization.

3.2 Using search functions

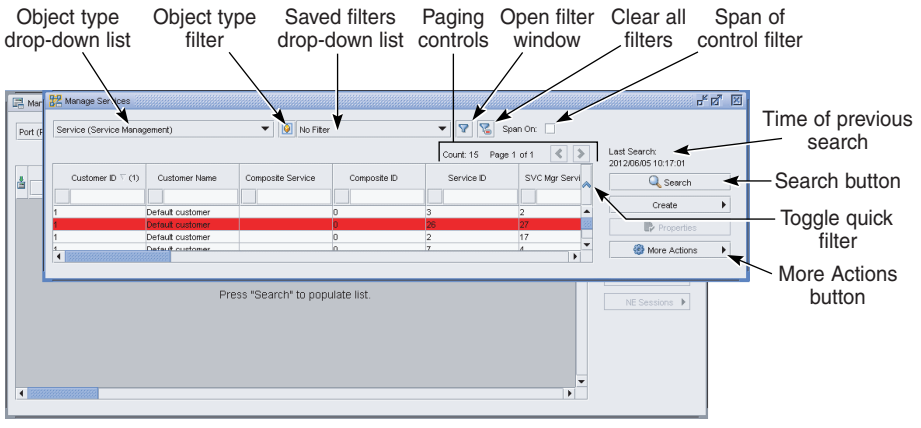
You can search for many types of objects using list forms, maps, and the navigation tree. For lists that do not populate automatically, the result panel displays the following message when you first open the list form:

```
Press "Search" to populate list.
```

After you perform a search, a list form or map enables you to manage the results, for example, view or modify or change object information, or delete objects. Figure 3-14 shows a filterable list form that displays the following information:

- number of returned search items
- time of the most recent search
- filter controls for refining the list of returned search items
- paging controls for browsing through multiple pages of returned search items

Figure 3-7 Filterable list form



If the number of search results exceeds the allowed limit, the 5620 SAM displays a dialog box that indicates the number of results returned. You can use filter options to refine the search criteria and limit the search results.

A search returns one page of results at a time. You can configure the number of items per page on the User Preferences form. The paging controls on a list form become active when the number of items returned exceeds the page limit. You can use these controls to move sequentially through the pages of listed information or jump directly to a specific page.

You can save and reuse multiple search filters in list forms and maps. Only the saved filters of the current object type and ancestor types are available. You can use an advanced filter form to refine the search criteria using literal values, and different types of operators, such as arithmetic and Boolean.



Note — A tab that lists timestamped information, such as the Statistics tab of a properties form, contains a default saved filter for statistics collected in the most recent time period, for example, the last hour. The time period depends on the type of object specified in the object type drop-down menu. See "To modify the default time period of statistics displayed by the Statistics Manager search filters" in the *5620 SAM System Administrator Guide* for more information.

See chapter 6 for information about creating map filters.

Using search filters

When you perform a search from a list form, you can configure filters. A filter is based on a combination of attributes, functions, and values. When searching for objects with an ID value, you can search based on LESS THAN, EQUAL TO, or GREATER THAN. For text-type parameters, you can use advanced search functions, such as EQUALS or CONTAINS. Consider the following.

- You can set filters based on letters, numbers, and special characters.
- The search filters are typically case-insensitive; a search on 'ABC' and 'abc' returns the same list. WILDCARD searches, however, are case-sensitive.

Table 3-1 describes the operation of available 5620 SAM search functions.

Table 3-1 Search functions

Operator	Description
APPROXIMATELY EQUAL	When set to APPROXIMATELY EQUAL, which applies to timestamp fields, such as the Last Time Detected field in the Alarm Window, the search returns only items that match the specified time criterion, which you can specify using 1m resolution.
BETWEEN	When set to BETWEEN, which applies to timestamp fields, such as the Last Time Detected field in the Alarm Window, the search returns only items with a timestamp that is within the specified range. Click on the Select icon beside the column heading filter field to specify a range.
CONTAINS	When set to CONTAINS, the search returns only items that match the entered value. For example, a Description CONTAINS search of 'AB' returns 'ABC Industries' and 'Calgary, AB'. Any empty CONTAINS search returns all items. This search parameter is not case sensitive.

(1 of 2)

Operator	Description
DOES NOT CONTAIN	When set to DOES NOT CONTAIN, the search returns only items that do not match the entered value. For example, a Service Name DOES NOT CONTAIN search of 'epipe' returns only services such as 'IES' services that do not contain 'epipe' as part of the service name. This search parameter is not case sensitive.
EQUALS	When set to EQUALS, the search returns only items that equal the value; for example, Administrative State set to Down.
GREATER OR EQUAL	When set to GREATER OR EQUAL, the search returns only items that have a value greater than or equal to the specified criteria.
GREATER THAN	When set to GREATER THAN, the search returns only items that have a value greater than the specified criteria.
IS BLANK	When set to IS BLANK, the search returns only items that do not have a value. For example, an Associated Template IS BLANK search of services returns services that have no associated template (where the associated template is blank).
IN THE PAST	When set to IN THE PAST, which applies to timestamp fields, such as the Last Time Detected field in the Alarm Window, the search returns only items that have a timestamp that is between the specified time and the present. Click on the clock icon beside the column heading filter field to specify a time criterion.
LESS OR EQUAL	When set to LESS OR EQUAL, the search returns only items that have a value less than or equal to the specified criteria.
LESS THAN	When set to LESS THAN, the search returns only items that have a value less than the specified criteria.
MATCHES ALL	When set to MATCHES ALL, the search returns only items that equal the property values selected; for example, if Monitored Access(es) Down and Site(s) Down are selected, the search returns only items that match all of the selected property values.
MATCHES ANY	When set to MATCHES ANY, the search returns only items that equal at least one of the property values selected; for example, if Monitored Access(es) Down and Site(s) Down are selected, the search returns only items that match one or more of each of the selected property values.
NOT EQUAL	When set to NOT EQUAL, the search returns only items that do not match the selected criteria.
WILDCARD	When set to WILDCARD, you can use the ? character as a single-character wildcard, and * as a multi-character wildcard. For example, a Description WILDCARD search of 'VPRN ?' returns 'VPRN 4' and 'VPRN 8', but not 'VPRN Texas'.

(2 of 2)

Searches using Boolean operators

You can perform advanced searches that use multiple criteria to obtain more precise results. Boolean operators are used to limit and expand searches to the criteria that are specified in the search expressions. Boolean operators can be nested to combine several search expressions into one search expression.

Table 3-2 lists and describes the Boolean search operators.

Table 3-2 Boolean search operators

Boolean operator	Description
AND	When set to AND, the search returns only items that meet all of the specified search criteria.
OR	When set to OR, the search returns only items that meet at least one of the specified search criteria.
NOT	When set to NOT, the search returns only items that do not meet the specified search criteria.

Invalid attributes or values

When a saved search filter contains attributes or values that are not available for the object being searched, the invalid attributes or values are displayed in red text in the filter window. As long as invalid attributes or values exist, the Save button of the filter window is disabled. When a filter with invalid attributes or values is applied, the invalid attributes are not evaluated. For information about using the filter window, see Procedure 3-25.

When a saved search filter contains an invalid attribute, the attribute, function, and value are all displayed in red text in the filter window. The attribute are is surrounded by "**". Both the attribute and value are displayed as a best effort string and may not be internationalized.

When an invalid attribute is selected, the Attribute drop-down is displayed a best effort string that may not be internationalized. If the attribute is not recognized, the Functions drop-down and the Value field display only the corresponding values that are displayed in the filter window. These values cannot be changed until a different attribute is chosen from the Attribute drop-down, at which point they are updated accordingly.

When a saved search filter contains only an invalid value, only the value itself is displayed in red text. The value is surrounded by "**" and may not be internationalized. The Value drop-down does not display a value, but is populated with valid values that can be used to update the filter.

When a saved search filter contains invalid attributes, the filter name is displayed in red text in the saved filters drop-down of a list form. When a filter with invalid attributes is applied from the saved filters drop-down, the invalid attributes are not evaluated. For information about using the saved filters drop-down list, see Procedure 3-35.

Preset filters

When a preset filter is ready to be applied, the saved filters drop-down menu displays an italicized No Filter. Opening the filter window displays the preset filter. Clicking on the Search button applies the filter, and clicking on the Clear All Filters button clears the filter.

Span of control filters

A 5620 SAM GUI user can filter the objects that a map or list form displays, based on the user span of control. By default, the GUI displays only the objects that are included in the View Access and Edit Access spans of the user.

Most 5620 SAM list forms contain a configurable Span On parameter. When the parameter is enabled, only the Edit Access span objects are displayed. On the current form only, the parameter setting overrides the global span of control filter setting on the User Preferences form. When the Span On parameter is displayed on a list form that allows filter creation, the associated filter form contains a drop-down menu that has the following options:

- Span: On—Only Edit Access span objects are displayed.
- Span: Off—View Access and Edit Access span objects are displayed.
- Span: User Preference—The User Preferences span filter setting determines the objects that are displayed.

The Span On parameter setting in a list form defaults to the User Preferences span filter setting. However, 5620 SAM topology maps, do not contain the Span On parameter; instead, topology maps automatically filter the NEs according to the User Preferences span filter setting.

See “Span of control” in the *5620 SAM System Administrator Guide* for more information about spans of control. See Procedure 3-19 for information about configuring the global span of control filter on the User Preferences form.

Equipment group filters

The equipment group filters allow you to search globally for new alarms, historical alarms, managed equipment objects, and managed service objects by equipment that is organized by topology group. See Procedure 6-28 for information about how to create a topology group.

The equipment group filter is created by choosing existing topology groups. The filters can be saved, modified, or deleted. See Procedures 3-37 and 3-38 for information about how to use the equipment group filters.

Equipment group filters can return up to 12 000 elements. If the limit is exceeded, the user is prompted to modify the filter to reduce the number of elements within the limit. Additionally, if you choose an equipment group filter that includes a topology group that has been modified since the filter was applied, an icon appears beside the equipment group filter drop-down list prompting you to press the Search button to update the filter.

Locating attributes on configuration forms

The find attribute function allows you to locate specific attributes on a configuration form.

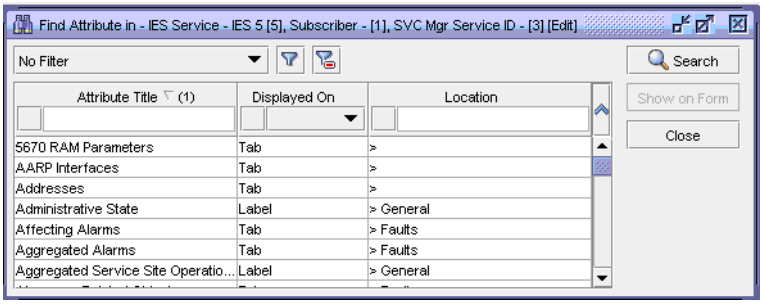


Note — In this context, attribute refers to the names of tabs, panels, or fields.

Using the Find button located in the bottom right of a configuration form, you can list the attributes in that form. The Find Attribute in list form includes the name, type, and location for all attributes on the configuration form. After you choose the attribute using one of the selection methods described in Procedure 3-27, the tab where the attribute resides appears and the attribute name is highlighted. After you close the list form, the attribute name returns to the default display color. Figure 3-8 shows the Find Attribute in list form.

Note — For configuration forms that can display multiple objects simultaneously, such as the service configuration forms, the search is performed only on the selected object.

Figure 3-8 Find Attribute in list form



3.3 Workflow to use the 5620 SAM GUI

1. Start the 5620 SAM GUI; see section 3.4.
2. Manage objects using the 5620 SAM main menu, contextual menus, navigation tree, and the alarm and map windows; see section 3.5.
3. Configure user preferences for the 5620 SAM GUI for one or more users, if required; see section 3.6.
4. Customize tabs on configuration forms, see Procedures 3-20 and 3-21.
5. Customize 5620 SAM GUI workspace elements to meet your operational requirements; see "5620 SAM custom workspaces".
6. Use list forms to perform filtered searches that return information, and optionally save the filters and listed information to files; see section 3.7.

3.4 5620 SAM GUI opening and closing procedures

The following procedures describe how to open and close the 5620 SAM GUI.

Procedure 3-1 To open a single-user GUI client on a Windows station

Note 1 — You can install more than one single-user client on a station, but you can run only one client instance of a release at a time. For example, a Release 10.0 client and a Release 11.0 client can be open at the same time, but not two Release 11.0 R1 clients.

Note 2 — To perform this procedure, you must be one of the following:

- the user who installed the client software
- a user with sufficient permissions on the client files and directories, such as a local administrator

1 Perform one of the following.

a Double-click on the 5620 SAM Client App icon on the Windows desktop.

b Start the client GUI using a web browser; perform the following steps.

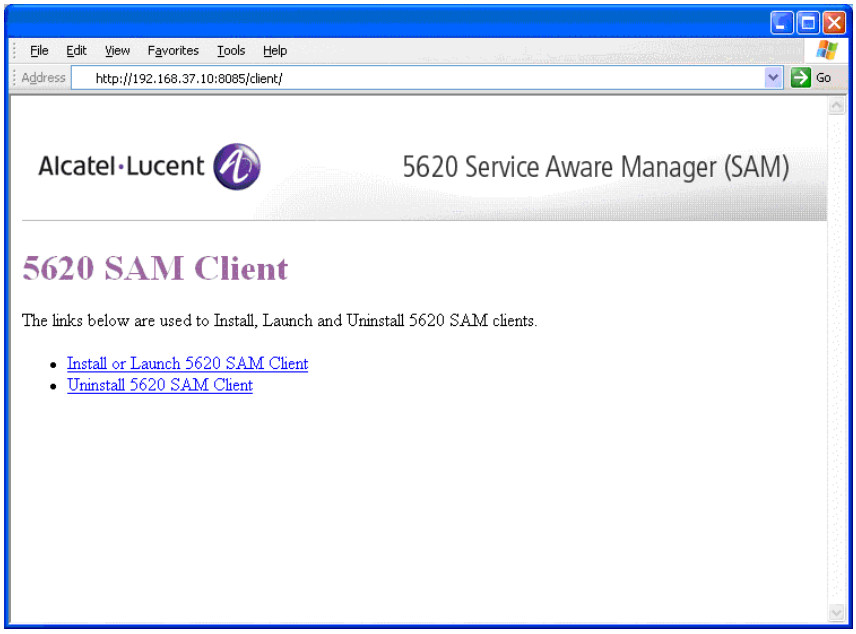
i Use the browser to open one of the following URLs:

- http://*server*:8085/client, if SSL is not enabled
- https://*server*:8444/client, if SSL is enabled

where *server* is the IP address or hostname of the 5620 SAM main server

The page shown in Figure 3-9 is displayed.

Figure 3-9 5620 SAM client page



ii Click on the “Install or Launch 5620 SAM Client” link.

iii If you did not use a web browser to install the client, a form opens and prompts you for the client installation location. Use the form to specify the client installation directory, for example, C:\5620sam\client.

c Start the client GUI using a CLI; perform the following steps.



Note — Using a CLI to start the client GUI allows you to specify one or more client startup options.

i Open a command window.

ii Navigate to the 5620 SAM client installation directory. Enter the following commands in the order shown:

drive_ID ↵

cd *install_dir*\nms\bin ↵

where
drive_ID is the drive on which the 5620 SAM client is installed, for example, C:
install_dir is the 5620 SAM client installation location, typically \5620sam\client

iii Enter the following to start the 5620 SAM client using one or more startup options:

nmsclient.bat *option1 option2 ... optionN* ↵

where *option1 option2 ... optionN* represents one or more of the startup options listed in Table 3-3

For example, to force a client update, enter the following:

nmsclient.bat update ↵

Table 3-3 5620 SAM client startup options for Windows

Option	Description
nms_version	Displays the client software version
baseLocale	Starts the client using the base OS locale for string resources such as language, number, date, and time formats
secure	Starts the client using HTTPS to connect to the server
server <*server*:*port*;*server*:*port*...>	Starts the client and specifies the 5620 SAM servers that the client is to check for an update where *server* is an IP address or a DNS name *port* is an HTTP or HTTPS port on the server
update	Starts the client and forces the download and installation of the updated client files. This overrides the local client configuration to ensure that the client and server configurations match. This option is useful for restoring a corrupted client installation. You can restore local configuration variances after the update.

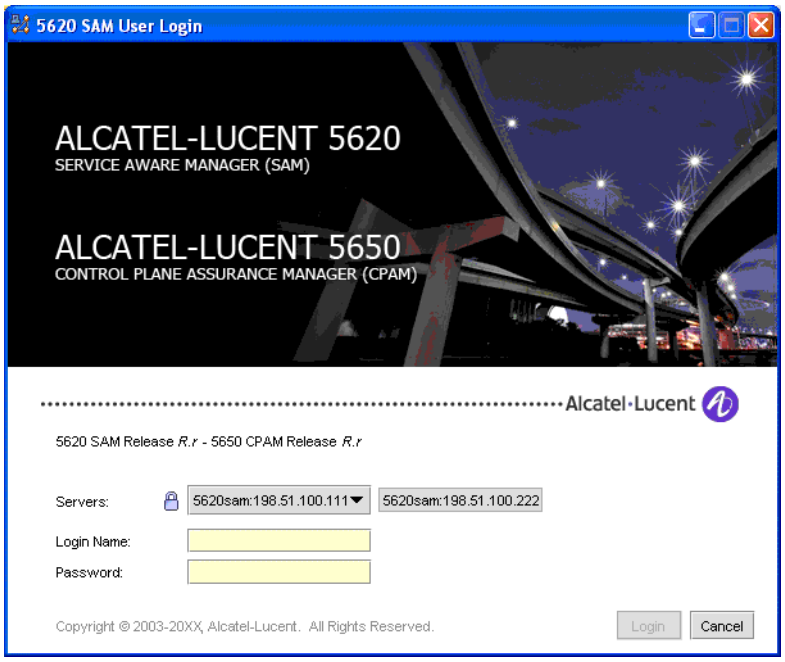
(1 of 2)

Option	Description
retryCount	Starts the client and specifies the number of times to attempt to download a client update
noupdate	Starts the client without performing an update. This option is useful for preserving a specific client configuration that differs from the server configuration.
keepConfig	Starts the client and performs an update, but does not permit the overwriting of the nms-*.xml configuration files in the *install_dir*\nms\config directory, where *install_dir* is the 5620 SAM client installation directory, typically C:\5620sam\client After this option is specified, it remains in effect until the client is started using the "update" option, which then remains in effect.
keepSpecified	Specifies that the files listed in *install_dir*\nms\config\keepFile.txt are not to be overwritten during a client update, where *install_dir* is the 5620 SAM client installation location, typically C:\5620sam\client The keepFile.txt file must contain only one file entry per line, and each entry must be an absolute file path.
connectTimeout [*timeout*]	Specifies a timeout value, in ms, that the client uses for a download-server connection attempt. If the client cannot connect to a server within the timeout period, the operation is aborted. The default is 3000, which specifies 3s. The maximum connection timeout in Windows is 20s.
readTimeout [*timeout*]	Specifies a timeout value, in ms, that the client uses for a download-server file read attempt. If the client cannot obtain a server response to a file request within the timeout period, the file request is aborted. The default is 3000, which specifies 3s. The maximum read timeout in Windows is 20s.
help	Displays the nmsclient.bat usage information and options

(2 of 2)

The 5620 SAM client login form opens. If SSL is enabled, the form displays a padlock icon, as shown in Figure 3-10.

Figure 3-10 Client GUI login form



2 Choose the appropriate 5620 SAM main server from the Server drop-down list.



Note — To display multiple server options in the Server drop-down list, you must configure the client to support multiple server options. See "To configure the display of optional servers on a 5620 SAM client GUI login form" in the *5620 SAM System Administrator Guide* for information.

3 Enter the required Login name and Password information.



Note 1 — If this is the first time that a client connects to the server, you must use admin as the Login Name. Contact your Alcatel-Lucent technical support representative for the default 5620 SAM user account information.

Note 2 — The login name and password used depend on whether client GUI users are authenticated locally or remotely, as determined by the system administrator. Use the login name and password provided by your system administrator.

4 Click on the Login button. The 5620 SAM GUI opens.

5 If the 5620 SAM server is at a higher major release level than the client, the auto-update function may display a dialog box that asks whether you need to remove an older version of JRE. If this occurs, perform one of the following.

- **a** If there is no longer a need for the client to connect to a main server at the older 5620 SAM release level, click on the Yes button. The older JRE version is removed.
- **b** If the client is required for connecting to a main server at the older 5620 SAM release level, click on the No button. The older JRE version is retained.

If you have trouble opening the GUI, see the *5620 SAM Troubleshooting Guide*.

Procedure 3-2 To open a single-user GUI client on a RHEL or Solaris station

Note 1 — You can install more than one single-user client on a station, but you can run only one client instance of a release at a time. For example, a Release 10.0 client and a Release 11.0 client can be open at the same time, but not two Release 11.0 R1 clients.

Note 2 — To perform this procedure, you must be one of the following:

- the user who installed the client software
- another user who has read, write, and execute permissions on the client files and directories

1 Perform one of the following.

a Double-click on the 5620 SAM Client App icon on the desktop.

b Start the client GUI using a web browser; perform the following steps.

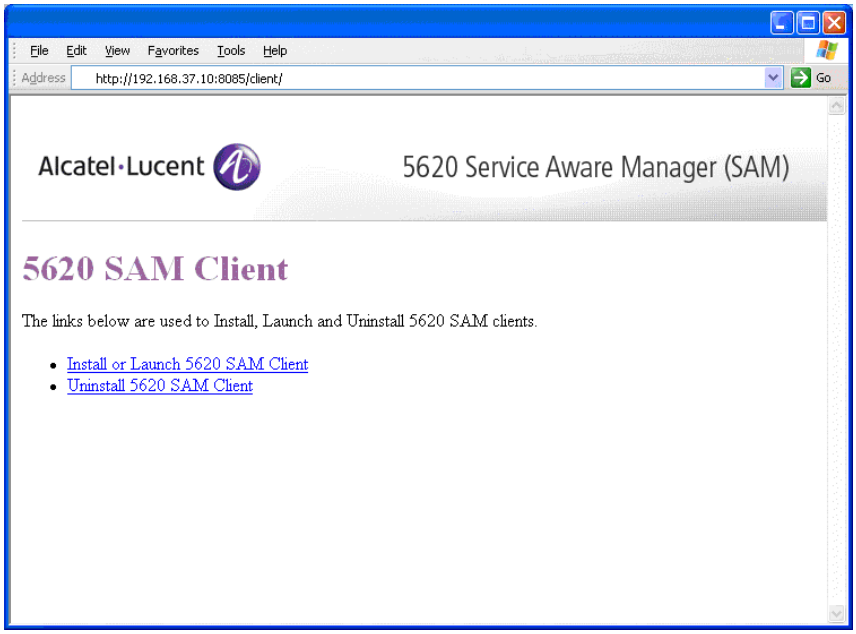
i Use the browser to open one of the following URLs:

- http://*server*:8085/client, if SSL is not enabled
- https://*server*:8444/client, if SSL is enabled

where *server* is the IP address or hostname of the 5620 SAM main server

The page shown in Figure 3-11 is displayed.

Figure 3-11 5620 SAM client page



ii Click on the “Install or Launch 5620 SAM Client” link.

iii If you did not use a web browser to install the client, a form opens and prompts you for the client installation location. Use the form to specify the current client installation directory, for example, /opt/5620sam/client.

c To start the client GUI using a CLI, perform the following steps.



Note — Using a CLI to start the client GUI allows you to specify one or more client startup options.

i Open a bash console window on the client station.

ii Enter the following to navigate to the 5620 SAM client installation directory:

```
cd install_dir/nms/bin ↵
```

where *install_dir* is the 5620 SAM client installation location, typically /opt/5620sam/client

iii To specify one or more client startup options, enter the following:

```
./nmsclient.bash option1 option2 ... optionN ↵
```

where *option1 option2 ... optionN* represents one or more of the startup options listed in Table 3-4

For example, to force a client update, enter the following:

```
./nmsclient.bash update ↵
```

Table 3-4 5620 SAM client startup options for RHEL and Solaris

Option	Description
nms_version	Displays the client software version
baseLocale	Starts the client using the base OS locale for string resources such as language, number, date, and time formats
secure	Starts the client using HTTPS to connect to the server
server <*server*:*port*;*server*:*port*...>	Starts the client and specifies the 5620 SAM servers that the client is to check for an update where *server* is an IP address or a DNS name *port* is an HTTP or HTTPS port on the server
update	Starts the client and forces the download and installation of the updated client files. This overrides the local client configuration to ensure that the client and server configurations match. This option is useful for restoring a corrupted client installation. You can restore local configuration variances after the update.
retryCount	Starts the client and specifies the number of times to attempt to download a client update

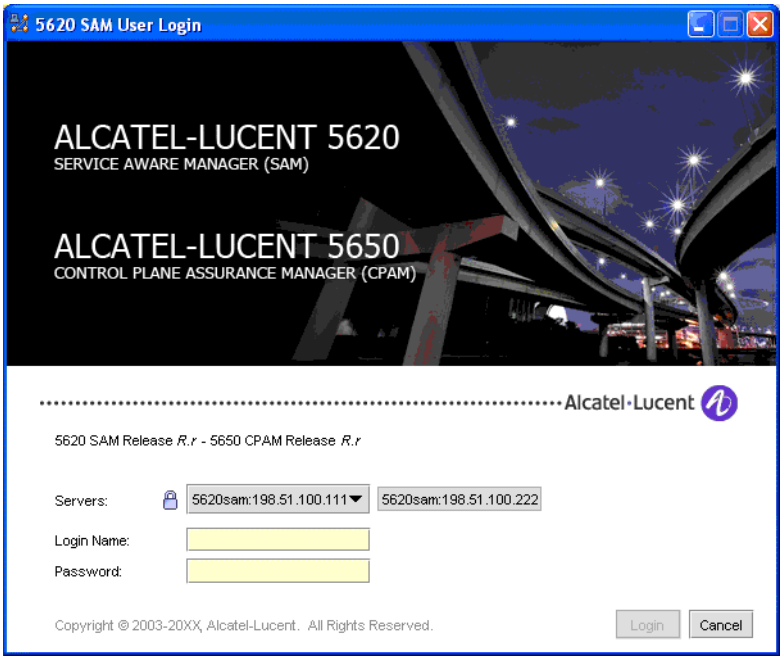
(1 of 2)

Option	Description
noupdate	Starts the client without performing an update. This option is useful for preserving a specific client configuration that differs from the server configuration.
keepConfig	Starts the client and performs an update, but does not permit the overwriting of the nms-*.xml configuration files in the *install_dir*/nms/config directory, where *install_dir* is the 5620 SAM client installation directory, typically /opt/5620sam/client After this option is specified, it remains in effect until the client is started using the "update" option, which then remains in effect.
keepSpecified	Specifies that the files listed in *install_dir*/nms/config/keepFile.txt are not to be overwritten during a client update, where *install_dir* is the 5620 SAM client installation location, typically /opt/5620sam/client The keepFile.txt file must contain only one file entry per line, and each entry must be an absolute file path.
connectTimeout [*timeout*]	Specifies a timeout value, in ms, that the client uses for a download-server connection attempt. If the client cannot connect to a server within the timeout period, the operation is aborted. The default is 3000, which specifies 3s.
readTimeout [*timeout*]	Specifies a timeout value, in ms, that the client uses for a download-server file read attempt. If the client cannot obtain a server response to a file request within the timeout period, the file request is aborted. The default is 3000, which specifies 3s.
help	Displays the nmsclient.bash usage information and options

(2 of 2)

The 5620 SAM client login form opens. If SSL is enabled, the form displays a padlock icon, as shown in Figure 3-12.

Figure 3-12 Client GUI login form



2 Choose the appropriate 5620 SAM main server from the Server drop-down list.



Note — To display multiple server options in the Server drop-down list, you must configure the client to support multiple server options. See "To configure the display of optional servers on a 5620 SAM client GUI login form" in the *5620 SAM System Administrator Guide* for more information.

3 Enter the Login name and Password information required for the server.



Note 1 — If this is the first time that a client connects to the server, you must use admin as the Login Name. Contact your Alcatel-Lucent technical support representative for the default 5620 SAM user account information.

Note 2 — The login credentials that are required depend on whether local or remote user authentication is used for the GUI client. Use the login name and password provided by your system administrator.

4 Click on the Login button. The 5620 SAM GUI opens.

5 If the 5620 SAM server is at a higher major release level than the client, the auto-update function may display a dialog box that asks whether you need to remove an older version of JRE. If this occurs, perform one of the following.

a If there is no longer a need for the client to connect to a main server at the older 5620 SAM release level, click on the Yes button. The older JRE version is removed.

b If the client is required for connecting to a main server at the older 5620 SAM release level, click on the No button. The older JRE version is retained.

If you have trouble opening the GUI, see the *5620 SAM Troubleshooting Guide*.

Procedure 3-3 To open a client GUI through a client delegate server

Perform this procedure to open a 5620 SAM client GUI using the 5620 SAM client delegate software on another station.

1 If you are not in the same physical facility as the client delegate server, log in to the facility using the appropriate access tool, for example, a Citrix gateway.

2 Log in to the client delegate server station.



Note — To specify a client startup option that updates the client software or configuration on a client delegate server, you must be logged in as one of the following users, or the update fails:

- on a RHEL or Solaris station—samadmin
- on a Windows station—the user who installed the client delegate server software, or a local administrator

3 If the client delegate server is installed on a RHEL or Solaris station, redirect the display to the station that you are using, if required. See the appropriate OS documentation for information.

4 Perform one of the following to open the GUI.

a Perform Procedure 3-1 if the client delegate server is on a Windows station.

b Perform Procedure 3-2 if the client delegate server is on a RHEL or Solaris station.

Procedure 3-4 To change to a different 5620 SAM client GUI user

Perform this procedure to change which 5620 SAM user is currently logged in to the client GUI.

1 Choose Application→Switch User from the 5620 SAM main menu. A dialog box appears.

2 Click on the Yes button. The GUI restarts and displays the login form.

3 Log in using the required credentials. The client GUI opens.

Procedure 3-5 To close the 5620 SAM GUI

1 Choose Application→Exit from the 5620 SAM main menu. A dialog box appears.

2 Click on the Yes button. The GUI application closes.

3.5 Basic 5620 SAM GUI operation procedures

The following procedures describe how to navigate and operate the 5620 SAM GUI.

Procedure 3-6 To open or close a main window

The following main GUI elements are displayed in windows:

- navigation tree
- topology map
- Alarm Window

By default, the navigation tree window appears at the left side of the GUI, the topology map window at the right, and the Alarm Window at the bottom.

1 To open a new window, or re-open a window that is closed, perform one of the following:

   a Click on the toolbar icon. If the toolbar or icon is not displayed, you can restore the toolbar; see Procedure 3-19.

   b Choose Application→*window_name* from the main menu, where *window_name* is the name of the window that you need to open.

   c Use the shortcut keys; see "Shortcut keys" in section 3.1.

2 To close a window, perform one of the following:

   a Click on the X icon in the upper right corner of the window.

   b Right-click on the taskbar button for the window you need to close and choose Close from the contextual menu.

Procedure 3-7 To close one or all open forms



Note — When there is unsaved information on a form, you are prompted to save the changes before you close the form.

1 To close a form, perform one of the following.

   a Click on the X in the top-right corner of the form.

   b Click on the Close button.

   c Right-click on a form button on the taskbar and choose Close from the contextual menu.

2 To close all open forms, choose Window→Close All Internal Windows or Close All External SAM Windows from the 5620 SAM main menu.



Note — When you close all internal windows, the navigation tree, topology map, Alarm Window, and any other open windows are closed. See Procedure 3-6 for information about how to re-open windows.

Procedure 3-8 To show or hide a window or form

1 To hide a window or form, perform one of the following:

   a Click on the minimize icon in the upper right corner of the window or form.

   b Click on the taskbar button for the window or form that you need to hide.

2 To move a hidden window or form to the foreground, perform one of the following:

   a Click on the taskbar button for the window or form that you need to move to the foreground.

   b Choose Window→*window_name* from the main menu, where *window_name* is the name of the window or form that you need to move to the foreground.

   c Use the shortcut keys. For more information, see "Shortcut keys" in section 3.1.

Procedure 3-9 To arrange windows and forms

You can optimize the workspace in the SAM GUI by arranging windows and forms.

1 To move a window or form manually, click and drag on the titlebar of the window or form.

2 To resize a window or form, hover over the border of the window or form until the double arrow appears, and click and drag the border.

3 To arrange multiple open forms so that they overlap, choose Window→Cascade from the 5620 SAM main menu. The forms are displayed in the top left of the GUI with the form that is farthest to the right in the foreground.



Note — When forms are arranged using the Cascade and Tile options, the main windows also display in the same arrangement as the forms.

4 To arrange multiple open forms so that they do not overlap, perform one of the following.

   a Choose Window→Tile Vertical from the 5620 SAM main menu. The forms are displayed beside each other.

   b Choose Window→Tile Horizontal from the 5620 SAM main menu. The forms are displayed above each other.

   c Choose Window→Tile Square from the 5620 SAM main menu. The forms are displayed beside and above each other to fill the GUI workspace.

5 To restore windows to their preferred settings, choose Window→Reset to Preferred Sizes from the 5620 SAM main menu.

Procedure 3-10 To move a window or form to an external window

A window or form in the GUI can be moved from the main workspace and managed as an external window; for example on a second monitor, if available. See "External windows" in section 3.1.

1 Click to select the window or form to move to an external window.

2 Perform one of the following:

   a Choose Window→Move to External Window from the 5620 SAM main menu.

   b Right-click on the titlebar of the selected window, and choose Move To External Window from the contextual menu.

3 Click on the titlebar of the window or form and drag to the external monitor, if available.



Note — An external window or form cannot be moved back to the 5620 SAM GUI. You must close the external window and re-open the window or form in the 5620 SAM GUI.

Procedure 3-11 To send a text message to other 5620 SAM users

You can send text messages to another 5620 SAM user or to all active users logged into the 5620 SAM.

1 Choose Application→Text Message from the 5620 SAM main menu. The Text Message window opens.

2 Enter the text message in the text area.

3 Click on the Send To... button. The Select Sessions form opens.

4 Configure the filter criteria to create a filtered list of GUI client sessions, if required.

5 Click on the Search button. A list of active GUI client sessions is displayed.

6 Perform one of the following:

a To choose a single user, click on a GUI client session.

b To choose all GUI client sessions, press CTRL+A

c To choose non-consecutive GUI client sessions, click on a session and press CTRL and choose another session.

7 Click on the OK button. The text message is sent to the specified clients. Messages are uniquely identified with the Client ID number of the sender. You can click on the reply button to reply back to the sender.

Procedure 3-12 To use menus, the toolbar, or shortcuts

1 Start the 5620 SAM GUI.

2 Perform one of the following to open an object.

a Choose an option from the 5620 SAM main menu. An icon for the menu option is displayed beside the option text.

b Click on the menu option icon in the toolbar. You can scroll over a toolbar icon to view a tool tip that describes the icon's function. See Procedure 3-19 for information about configuring or hiding the toolbar.

c Use the shortcut keys. Simultaneously press ALT-*key* where *key* is the underlined letter in the menu item. For example, ALT-P opens the Policies menu. The menu item must be displayed for the shortcut key to work.



Note — Using the CTRL+F4 key to close a form or window may cause problems if the parent form is open. Alcatel-Lucent recommends that to close a form or window, you use the Close button and respond to the subsequent prompt, or click on the X button in the top right corner of the form or window.

Procedure 3-13 To use menus, windows, and forms to configure or view parameters

1 Start the 5620 SAM client GUI.

2 Open a configuration form using one of the following methods.

a Double-click on the lowest-level navigation tree object to open the object properties form. When you double-click on an object that has child objects, the child object is revealed; when you double-click on an object that has no child objects, the object properties form opens.

b Choose the appropriate 5620 SAM main menu or submenu option.

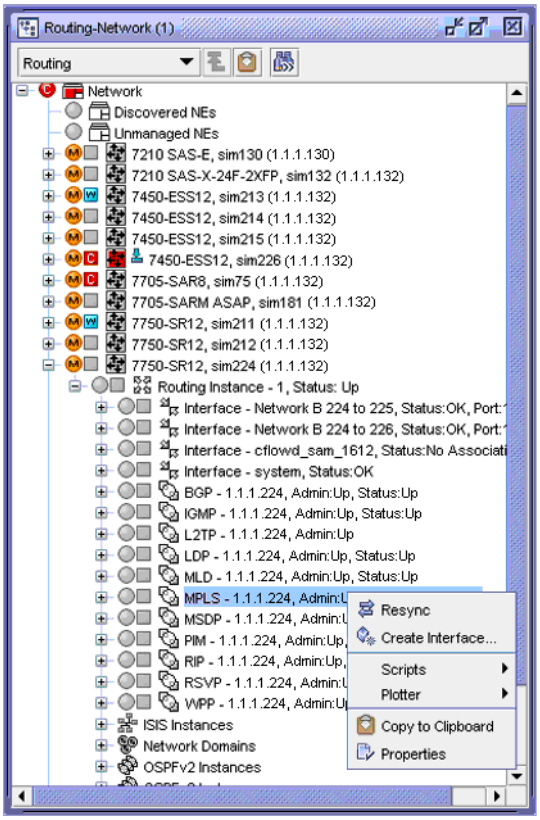
c Double-click on an object, for example, a customer in a list of customers.

d Click on the task bar button that represents the form.

e Right-click on an object in the navigation tree or Alarm Window and choose the appropriate option from the contextual menu.

Figure 3-13 shows an example of a right-click contextual menu in the navigation tree.

Figure 3-13 Right-click contextual menu example



The appropriate form opens.

3 Configure or view the parameters on the form, as required, using the following methods.

Note — A parameter that has a yellow background is mandatory and must be configured before you can go to the next form or apply the changes on the current form.

a Enter information beside the parameter, as appropriate. For example, type in text to configure the Description parameter.

b Use the drop-down menu to choose an option from a list. For example, choose Access as the port mode on a port configuration form.

c If the configuration form is a step form, follow the form prompts.

d Double-click an object in a row to open a new view or set of configurations. For example, from a list of ports double-click on a row to open the configuration form for that port.

e Right-click on an object in the navigation tree to display additional contextual menu choices, as shown in Figure 3-13.

See the *5620 SAM Parameter Guide* for a list of the configurable parameters.

4 Click on the Apply button to save the configuration changes without closing the form.

5 Click on the appropriate button to complete the configuration.

a Click on the OK button to save the changes and close the form, if the form is other than a step form.

b Click on the Finish button to save the changes in a step form.

c Click on the Turn Up button to activate the object. If the Turn Up button is not visible, click on the More Actions button and choose Turn Up.

d Click on the Shut Down button to deactivate the object. If the Shut Down button is not visible, click on the More Actions button and choose Shut Down.

e Click on the Cancel button to close the form without saving the changes.

f Click on the Close button to close the form without saving the changes.



Note — Using the CTRL+F4 key to close a form or window may cause problems if the parent form is open. Alcatel-Lucent recommends that to close a form or window, you use the Close button and respond to the subsequent prompt, or click on the X button in the top right corner of the form or window.

g Click on the Resync button to ensure that the 5620 SAM and managed devices are synchronized. Resynchronization does not affect the contents of the historical statistics database.

Procedure 3-14 To use the Parameter Search Tool

The Parameter Search Tool contains information about parameters and configuration forms in the 5620 SAM. See "Parameter Search Tool" in section 3.1.

1 Choose Help→User Documentation from the 5620 SAM main menu. A browser window opens with the User Documentation Index displayed.

2 Click on the Parameter Search Tool link. Alternatively, in the Contents panel, expand the Parameter Guide book and click on Parameter Search Tool.

3 Perform any of the following:



Note — You can choose the options from the Contents panel or the display panel.

a Search for a parameter or form name.

i Click on Search parameter and form names. The Search parameter and form names page is displayed.

ii Enter a term in the Search Term field.

iii Choose an option from the Please select a Type drop-down menu.

iv Click on the Search button. A list of results is displayed.

v Choose an entry. Information about the form that is associated with the entry is displayed.

b Display a configuration form from the list.

i Click on Configuration forms. A list of configuration form names is displayed.

ii Choose a configuration form name from the list. Information about the form is displayed.

4 In the Tabs section, click on a tab name to display only the parameters for that tab.

5 Click on a parameter name to view information about that parameter.



Note 1 — To manage the display of information, hover over the MENU box and then choose from the options that appear.

Note 2 — Some parameters are configured from a list of options (called enumerations). To view parameter enumerations, click on the linked text in the “type” field and view the entry for the linked text.

Procedure 3-15 To use the 5620 SAM clipboard

Perform this procedure to copy property form identifier links for objects in the navigation tree or list forms. See 5620 SAM clipboard in section 3.1. For information about using the clipboard to create physical links, see Procedure 6-33.

1 To copy objects to the clipboard from the Equipment view of the navigation tree:

   a Select one or more objects from the equipment list.

   b Click on the Copy to Clipboard icon on the navigation tree window toolbar.

2 To copy objects from a generated or displayed list:

   a Select the object or objects to copy from the list.

   b Click on the Copy to Clipboard button on the list form.



Note — Each time the Copy to Clipboard function is used, the previous clipboard contents are replaced.

Procedure 3-16 To copy a property form to the clipboard

A property form identifier link is a unique internal address that the 5620 SAM assigns to a form or window. For example: *sam://topologyGroup:Network-DiscoveredNes*.



Note — Each time the Copy Property Form Identifier function is used, the previous clipboard contents are replaced.

1 Open a property form and a tab, if required.

2 Perform one of the following:

   a Choose the form and tab that you need to copy and choose Application→Copy Property Form Identifier from the 5620 SAM main menu. The property form identifier link is copied to the clipboard.

   b Choose the form and tab that you need to copy, right-click on the open property form titlebar and choose the Copy Property Form Identifier function. The property form identifier link is copied to the clipboard.

   c Choose the form and tab that you need to copy, right-click on any tab in an open property form and choose the Copy Property Form Identifier function. The tab on the property form identifier link is copied to the clipboard.

3 Close the property form.

Procedure 3-17 To open a property form copied to the clipboard

1 Choose Application→Go To Property form from the 5620 SAM main menu. The Go To Property Form window opens.

2 Click on the Paste button. The last-copied property form identifier link is copied to the clipboard. For example, the tab location on the properties form that was last opened, appears in the label area.



Note — If the clipboard contains multiple objects, only the first object in the clipboard list is pasted.

3 Perform one of the following:

a Click on the OK button. The Go To Property Form window closes and the tab location on the properties form copied to the clipboard, opens.

b Click on the Apply button. The tab location on the properties form copied to the clipboard, opens.

Procedure 3-18 To open property forms from the clipboard menu

1 Choose Application→Clipboard from the 5620 SAM main menu. The Clipboard window opens.

2 Select an object from the Clipboard window. Only one object can be selected.

3 Click on the View Object button. The form for the selected object opens.

3.6 5620 SAM GUI user preferences configuration procedures

The following procedures describe how to configure user preferences for the 5620 SAM GUI.

Procedure 3-19 To configure 5620 SAM user preferences

1 Choose Application→User Preferences from the 5620 SAM main menu. The User Preferences form opens with the General tab displayed.

Table 3-5 lists the tasks that can be configured using the User Preferences form and the location of more information, if applicable. The user preferences are listed by the functional tabs as they appear on the User Preferences form.

Table 3-5 User Preferences tasks and location

Task	See
General tab	
Show Toolbar: To show or hide the toolbar icons under the main menu, including the default set of toolbar icons and a custom workspace set of toolbar icons. You can create a unique set of toolbar icons with each custom workspace.	—
Default Client Time Zone: To configure the default client time zone.	—
Alarm Window panel: To configure the user preferences in the alarm window: • Turn on Audible Alarms • Show Alarm Flags • Show Correlated Alarms by Default. You can also configure the display of correlated alarms from the Alarm window • Enable or disable the display of alarmed equipment in navigation trees for the View Alarmed Object function.	Procedures 31-9, 31-10, 31-11, and 31-12
Configuration Forms panel: To configure user preferences to: • Suppress Containing Window Warning • Suppress Template Generation Message • Suppress Template Execution Warning • Debug STM Mode:To access test objects that are available in the STM • Enable Confirmation for Bulk Change Actions: To specify whether the 5620 SAM displays a confirmation message when an operator initiates a bulk change operation	—
Topology Windows panel: To configure user preferences to: • Suppress Service and Composite Service Map Load Warning • Overlay Type	—
Auto ID Generation panel: To configure user preferences to Access Interface Encap Value (Dot1q only).	—

Listing Forms panel: To configure user preferences to:
• Specify # of items Per Page: To specify the maximum number of objects to display per page on a list form
• Apply User Span Of Control
  • By default, the GUI displays all objects that are in your View Access and Edit Access spans. Use the parameter to display frames that include list forms, maps, and the alarm window.
  • You can temporarily override the global filter setting in a list form or window using the Span On check box, and you can include your span of control in an advanced filter window.
  • You can perform searches using list forms and span of control filters.
  • Procedure 3-29 affects the GUI display of only the user who configures the Apply User Span of Control parameter, and not other users.
	—
	Procedure 3-29
	Section 3.2

Browser Path: To configure or reset the path to a web browser on your local station to access the Supervision Portal from the 5620 SAM main menu.	*5620 SAM Supervision Module User Guide*
Statistics Plotter tab	
To configure the real-time plot configuration user preferences for graphing statistics including: • Default Polling Interval (Seconds) • Maximum Data Retention Time (Seconds)	*5620 SAM Statistics Management Guide*
Script Management tab	

(1 of 2)

Task	See
To configure the script management and templates user preferences for the following: • Enable Command Helper: The Command Helper appears when you click on the designated command helper key in the Script Editor. • Command Helper Key: To identify the keyboard key that is used to access the Command Helper. • GUI Builder in the Editor: To enable or disable the Velocity GUI Builder which is used to create or modify Velocity properties, or test the generated UI.	*5620 SAM Scripts and Templates Developer Guide*
Workspaces tab	
To add or remove custom workspaces or change the sequence of the custom workspace in the Workspace Selector. You can also set a custom workspace as the default workspace. The Workspace Selector allows you to change from the default workspace to your custom workspace.	Procedure 4-6

(2 of 2)

2 Click on the OK button. A dialog box appears.

3 Click on the Yes button and close the User Preferences form.

Procedure 3-20 To customize tabs on configuration forms

You can display, hide, or reorder tabs on a configuration form to customize which tabs are visible for a specific object type.



Note — An administrator can configure the default behavior for custom tab configuration from the System Preferences form. See the *5620 SAM System Administrator Guide*.

1 Open the configuration form for any object.

2 Click on the tab selector on the right side of the form. A drop-down list of tabs is displayed.

3 Perform any of the following, as required:

a To display a hidden tab, choose a tab from the Hidden Tabs and click on the Move to Displayed Tabs button.

b To hide a displayed tab, choose a tab from the Displayed Tabs Order and click on the Move to Hidden Tabs button.

c To reorder a displayed tab, choose a tab and click on the Move Up or Move Down button until it is located at the desired location in the Displayed Tabs Order.



Note 1 — You can select and move multiple tabs.

Note 2 — Tab settings are specific to the selected object type. For example, if you open the Network Element (Edit) form for a 7705 SAR-H and hide all tabs except the General tab, then open the same form for a 9500 MPR, the form displays the General tab and may also display some 9500 MPR specific tabs.

Note 3 — At least one tab must be displayed on a form. If all tabs are moved to the Hidden Tabs, the Save Tab Settings button is disabled.

Note 4 — Mandatory tabs do not appear in the drop-down list of tabs, such as the TCA, Faults, and Deployment tabs.

4 Click on the Save Tab Settings button. The form updates with the specified custom tab configuration.



Caution — If you close the tab selector drop-down list without saving, all unsaved tab preferences are lost.



Note — The Find Attribute window lists all parameters on the form including parameters located on hidden tabs. If you need to temporarily display a parameter located on a hidden tab, click on the Show on Form button. The tab is temporarily displayed on the form.

5 Close the form.

Procedure 3-21 To temporarily display hidden tabs on configuration forms

You can temporarily display hidden tabs on a configuration form. Tabs that are displayed this way are hidden again when you close the form.

1 Open the configuration form for any object.

2 Perform one of the following:

a To temporarily display all hidden tabs, click on the Show All Tabs button on the right side of the form. The form displays all available tabs.



Note — If no available tabs are currently hidden, the Show All Tabs button is disabled.

b To temporarily display one hidden tab, perform the following:

i Click on the tab selector on the right side of the form. A drop-down list of tabs is displayed.

ii Choose a tab from the Hidden Tabs and double-click on it. The form displays the chosen tab.



Note 1 — Hidden tabs that are displayed temporarily are shown in italics under Displayed Tabs Order on the tab selector drop-down list.

Note 2 — If you click the Save Tab Settings button, all temporarily displayed tabs become permanent.

3 Close the form.

Procedure 3-22 To configure the current client time zone

Perform this procedure to specify which time zone the 5620 SAM client will use currently.

1 Click on the Current Client Time Zone button in the bottom right corner of the GUI. The Current Client Time Zone form opens.

2 Perform one of the following:

a Select Use Default Client Time Zone.

b Select Use Specific Client Time Zone and choose a time zone from the list.

3 Click on the OK button. The Current Client Time Zone form closes and a dialog box appears.

4 Click on the OK button.

3.7 5620 SAM GUI search procedures

The following procedures describe how to use the 5620 SAM client GUI to search for and display information.

Procedure 3-23 To monitor the 5620 SAM Task Manager

Perform this procedure to monitor your operational requirements. The Task Manager allows 5620 SAM operators to monitor the progress of operational tasks. Only 5620 SAM administrators can change task monitoring parameters. "To change the 5620 SAM Task Manager default settings", see the *5620 SAM System Administrator Guide* for more information.



Note — You can send the tasks that the Task Manager displays to a file using the OSSI findToFile method. See "Inventory retrieval" in the *5620 SAM XML OSS Interface Developer Guide* for more information.

1 Choose Application→Task Manager from the 5620 SAM main menu. The Task Manager form opens.

The All Users check box only appears for 5620 SAM administrators. If you are a 5620 SAM administrator or a user with an assigned administrator scope of command role, go to step 2 to monitor tasks for all users. Otherwise, go to step 3.

2 Enable the All Users check box to monitor operations that are performed in the 5620 SAM server by all 5620 SAM users. The default is Disabled.

3 Configure the task management filter to monitor the 5620 SAM operations, as required. For example, you can monitor operations based on the server start time, the elapsed time, the status of the operation, or by the user performing the operation.

4 Click on the Search button. Operations that meet the specified search criterion are displayed. The following appear in the Task Manager:

- all write operations that are performed from the 5620 SAM GUI; for example, when you click on the Apply or OK buttons
- all write operations that are performed using the OSSI
- some read operations; for example, when you click on the Resync or Collect All buttons



Note — The Task Manager automatically refreshes when the value of the autoRefreshInterval parameter is reached. The default is 20. You can also click on the Search button to refresh the list of tasks.

5 Double-click on a task to view more information about the task. The Task - Top Level form opens with the General tab displayed.

6 Click on the Tree tab to view a hierarchical display of the task and subtasks.

7 Click on the Sub-Tasks tab to view the subtasks of the task.

8 To view the 5620 SAM GUI or OSS user activity associated with a task, click on the User Activity button. If the User Activity button is not visible, click on the More Actions button and choose User Activity. The Activity form opens and displays additional information about the task. See "User activity logging" in the *5620 SAM System Administrator Guide* for more information.

9 Close the open forms, as required.

Procedure 3-24 To perform a simple search using column headings

1 Open a list form.

2 If available, choose an entry from the object drop-down list.



Note — If you click on the Search button without selecting a specific object type from the list, a default entry may be used.

3 If the filter has not been pre-populated, configure the filter criteria using the filter area of any column heading.



Note 1 — If you enter a value in a filter area of a column heading without specifying an operation from an operation drop-down menu, a default operation is automatically selected.

Note 2 — The operators listed below are available specifically for filtering a list by object timestamp. Each operator allows you to specify the time criteria. Click on the Select icon, if available, beside the column heading filter to specify a range.

- APPROXIMATELY EQUAL, which allows you to specify a time with 1m resolution rather than the 1ms timestamp resolution (default)
- IN THE PAST, which allows you to specify an amount of time before the current time as the filter range, for example, 3 hours after the current time
- BETWEEN, which allows you to specify a Start Time and End Time (If the start and end time are the same, the OK button is disabled.)

Note 3 — Selecting NONE in an operation drop-down menu clears the filter area of the associated column heading.

Note 4 — Clicking on the Toggle Quick Filter button toggles the visibility of the filter areas on or off.

Note 5 — The filter areas of the column headings are disabled if a filter was applied using the filter window, if the filter window is open, or if a saved filter was loaded using the saved filter drop-down list. See Procedure 3-25 for more information about performing an advanced search.

4 Click on the Search button. The results list is displayed based on the filter.

5 To refresh the search results using the currently defined filter, click on the Search button. If applied, the current filter is used even when the filter areas are hidden or closed.

6 Close the List Form.

Procedure 3-25 To perform an advanced search

1 Open a List Form.

2 Click on the Filter button at the top of the form. The filter window opens.



Note — The filter areas of the column headings in a List Form are disabled if a filter is applied using the filter window, if the filter window is open, or if a saved filter was loaded using the saved filters drop-down list. See Procedure 3-24 for more information about performing a simple search using column headings.

3 Configure the filter properties.

i Choose an item from the Attribute drop-down menu.

ii Choose an item from the Function drop-down menu.

iii Choose an item from the Value drop-down menu.

iv Choose a Boolean Operator from the Operators drop-down menu.

v Click on the Add button.

4 Do one of the following.

a To filter additional properties, repeat step 3.

b To modify the search filter, go to step 5.

c If you are finished filtering properties, go to step 6.

5 Modify the search filter, if required.

a Replace a Boolean operator.

i Select a Boolean operator in the summary area.

ii Choose an item from the Operators drop-down menu to replace the selected Boolean operator.



Note 1 — If an entire bracket is selected, all Boolean operators within are replaced at once.

Note 2 — If multiple filtered properties exist, replacing a Boolean operator wraps the properties associated with that operator in brackets.

b Exclude filtered properties.

i Select a filtered property in the summary area.

ii Click on the NOT button to exclude any matching entries from the search results.



Note 1 — If an entire bracket is selected, all filtered properties within are excluded at once.

Note 2 — Selecting an excluded property or a bracket and clicking on the NOT button includes the property or bracket again.

c Replace filtered properties.

i Select a filtered property in the summary area.

ii Configure the filter properties, as described in step 3.

iii Click on the Replace button.

d Delete filtered properties.

i Select a filtered property or a bracket in the summary area.

ii Click on the Delete button to remove the selected filtered properties from the search filter.



Note — Multiple filtered properties can be selected and deleted at once.

e Wrap filtered properties in brackets.

i Click the left mouse button and drag over multiple filtered properties in the summary area to select them.

ii Click on the brackets button to wrap the selected filtered properties in brackets.



Note 1 — Selecting properties that are already wrapped in brackets and clicking on the brackets button unwraps the selected properties.

Note 2 — Properties can only be wrapped or unwrapped if all Boolean operators contained within are matching.

6 Click on the Apply button or the OK button. The results list is displayed based on the filter.

7 If the filter window is open, click on the Close button. The filter window closes.

8 Close the List Form.

Procedure 3-26 To perform a search by specifying endpoints

Use the following procedure to find objects such as service tunnels, MPLS paths, VLAN paths and LSP paths by specifying endpoints.

1 Choose one of the following menu options from the 5620 SAM main menu:

- Manage→MPLS→Dynamic LSPs
- Manage→MPLS→Manual Bypass LSPs
- Manage→MPLS→Static LSPs
- Manage→MPLS→MPLS Paths
- Manage→MPLS→Static LSPs
- Manage→Service Tunnels
- Manage→VLAN→Paths

The Manage filter form opens.

2 Click on the Filter button. The filter window opens.

3 Choose Endpoints from the Select Filter Type drop-down menu. Endpoints is the default option.



Note — If a saved filter is selected or the filter areas of the column headings are populated, Advanced Filter is the default option.

4 Deselect the Any Source check box to pick a source IP address as a search filter. Otherwise, leave the Any Source check box selected to search by any source IP address.

5 Deselect the Any Destination check box to pick a destination IP address as a search filter. Otherwise, leave the Any Destination check box selected to search by any destination IP address.

6 Click on the Apply button. The results list is displayed based on the filter.

7 Click on the Close button to close the filter window.

8 Close the List Form.

Procedure 3-27 To locate an attribute on a configuration form

1 Open a configuration form.

2 Click on the Find button or press CTRL+F. The Find Attribute in list form opens and displays the attributes on the configuration form.

3 Configure the filter criteria and click on the Search button. A list of attributes is displayed.

4 Choose an attribute from the list and perform one of the following:

- **a** Click on the Show on Form button.
- **b** Double-click on the attribute row.
- **c** Press Enter.

On the configuration form, the selected name of the tab, panel, or field is highlighted and the associated tab is displayed.



Note 1 — If a tab is hidden on a form and you click on the Find button, you can choose a parameter from the list that appears in the hidden tab and click on the Show on Form button, the hidden tab is temporarily displayed.

Note 2 — For configuration forms that can display multiple objects simultaneously, such as the service configuration forms, the search is performed only on the selected object.

Procedure 3-28 To filter object types

When an object drop-down list contains more than 10 items, you may click on the Filter for Object Type button to refine your search.

1 Open a List Form.

2 Click on the Filter for Object Type button. The Select Object Type form opens.

3 Configure the filter criteria using the filter area of any column headings.



Note — You can click on the Filter button on the Select Object Type form to open the filter window. See Procedure 3-25 for more information about performing an advanced search.

4 Click on the Search button. The results list is displayed based on the filter.

5 Select an object from the list and click on the OK button. The Select Object Type form closes and the List Form reappears with the new Object Type selected in the Object Type drop-down.

Procedure 3-29 To filter using span of control

On some List Forms, you can create and save a span filter to display objects for your specific span of control. For example, if you need to see objects within the span of control that has been assigned to you, create a span filter. You can also configure user preferences to automatically filter out objects that are not in your span of control.

1 Open a List Form.

2 If available, choose an entry from the object drop-down list.

3 Do one of the following.

a To search using Span of Control from a List Form, go to step 4.

b To search using Span of Control from the filter window, go to step 5.

4 Click on the Span On check box. The results list is displayed based on the filter. Go to step 9.

5 Click on the Filter button. The filter window opens.

6 Choose an entry from the Span drop-down list.



Note — An entry from the Span drop-down list is selected based on the Span On check box on the List Form.

7 Click on the Apply button. The results list is displayed based on the filter and the Span On check box is updated.

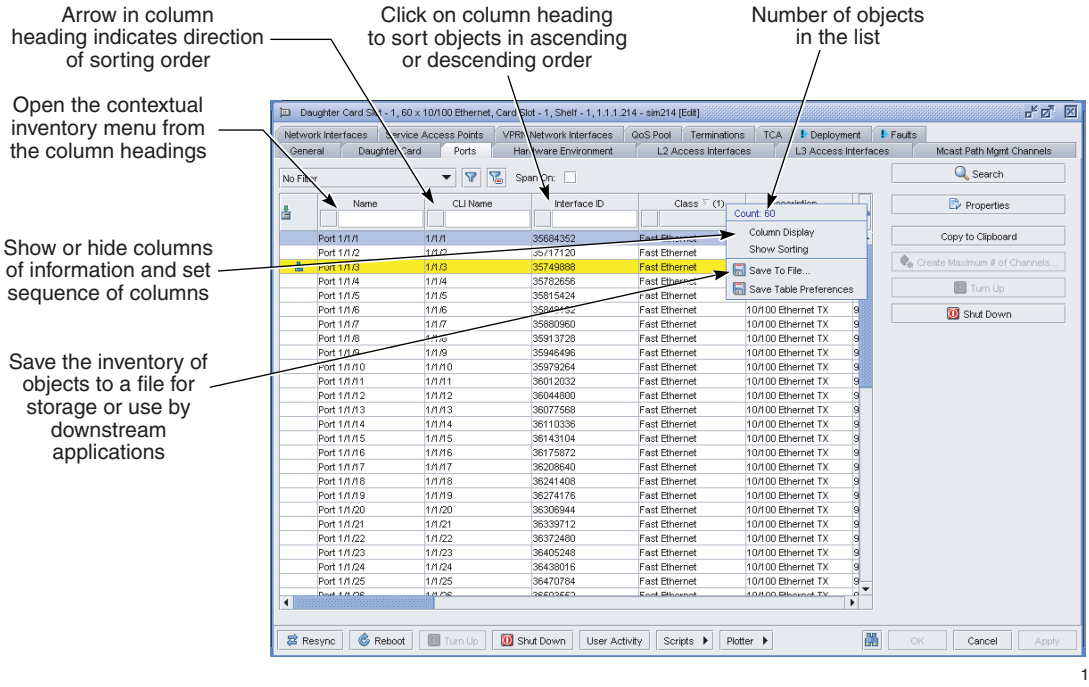
8 Click on the Close button. The filter window closes.

9 Close the List Form.

Procedure 3-30 To view and manage listed information

Many of the windows and forms are lists of network objects, for example, lists of ports displaying all the ports on a specific card. Figure 3-14 shows the major elements of a list.

Figure 3-14 List elements



17271

On most lists, you can:

- generate inventories of the listed data
- reorganize the information from most important to least important
- remove columns of data that are not of interest
- sort listed information in ascending or descending order

1 Generate a list.

2 Perform an action on the list.

a To generate an inventory of data, right-click on the list heading. The Count indicates the number of objects in the list.

b To remove columns from the table:

i Right-click on the column heading and choose Column Display from the contextual menu. The Column Display window appears.

ii In the Displayed on Table list box, choose the columns that you need to remove from the table and click the left arrow. The specified columns are moved to the Available for Table list box.

Note 1 — Columns that cannot be removed from the table are dimmed in the Displayed on Table list box.

Note 2 — There must be at least one column in a table.

iii To resequence the columns, go to step dii.

iv Perform one of the following.

- Click on the Apply button to apply the configuration changes without closing the form. The specified columns are removed from the table.
- Click on the OK button to apply the changes and close the Column Display window. The specified columns are removed from the table.
- Click on the Cancel button to close the Column Display window.

c To add columns to the table:

i Right-click on the column heading and choose Column Display from the contextual menu. The Column Display window appears.

ii In the Available for Table list box, choose the columns that you need to add to the table and click the right arrow. The specified columns are moved to the Displayed on Table list box.

iii To resequence the columns, perform step dii.

iv Perform one of the following:

- Click on the Apply button to apply the configuration changes without closing the form. The added columns appear in the table.
- Click on the OK button to apply the changes and close the Column Display window. The added columns appear in the table.
- Click on the Cancel button to close the Column Display window.

d To reorganize the information:

i Right-click on the column heading and choose Column Display from the contextual menu. The Column Display window appears.

ii In the Displayed on Table list box, choose the name of the column that you need to move.

iii Click on the up and down arrows to move the column to the appropriate location in the table.



Note — You can move multiple columns simultaneously by choosing more than one column name before you click on the arrows.

iv Perform one of the following.

- Click on the Apply button to apply the configuration changes without closing the form. The columns appear on the table in the new sequence.
- Click on the OK button to apply the changes and close the Column Display window. The columns appear on the table in the new sequence.
- Click on the Cancel button to close the Column Display window.



Note — You can also resequence information by clicking on a column, dragging the column to the right or left, and dropping the column in the appropriate location.

e To sort data based on a column in ascending or descending order, click on the column heading. The down or up arrow changes and indicates the sequence in which the data is sorted.

f To sort data based on multiple columns, perform one of the following:

i Right-click on a column heading and choose Show Sorting from the contextual menu. The Show Sorting form opens. Choose the one or more properties from the Available for Sorting panel and click on the right arrow button. The properties appear in the Used for Sorting panel. Click on the Sort Ascending or Sort Descending, as required.

ii Click on the column heading of the first column by which you need to sort. Press and hold CTRL and click on one or more additional columns in the sequence in which you need to sort the data. The sort sequence appears in brackets after the column name. To change the direction of the sort, click on the heading of any of the selected columns while pressing CTRL.



Note — To navigate quickly through a long sorted list, type a letter to move directly to the first item in the list that starts with that letter.

Table 3-6 describes the order in which different types of data are sorted from the top of the column to the bottom, based on the direction of the arrow in the column header. Figure 3-15 shows an example of information sorted in a column according to the down arrow in the column header.

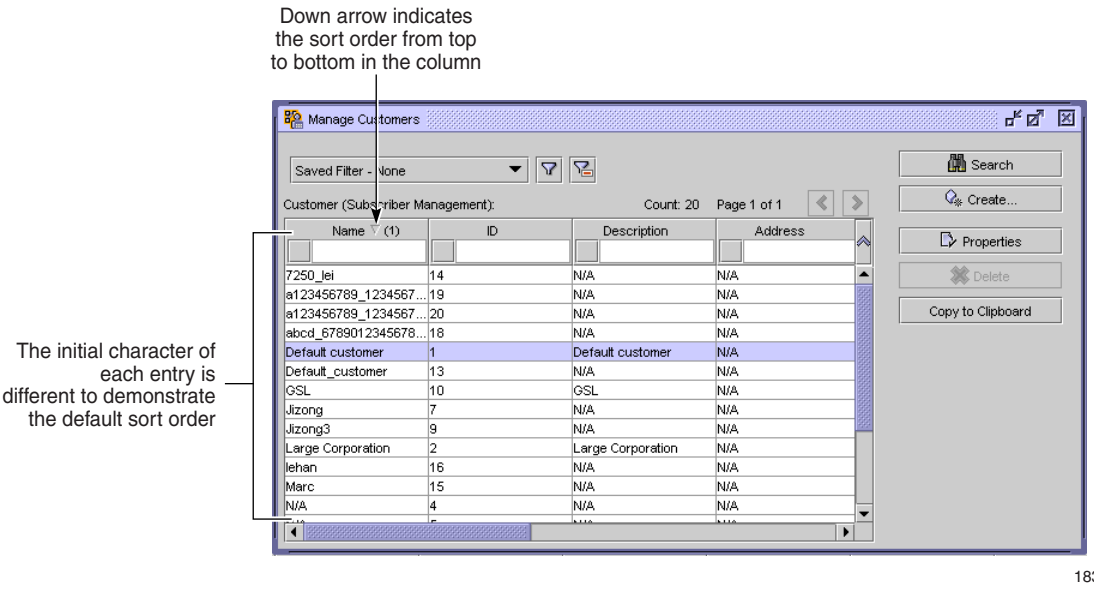
Table 3-6 Sorting listed information

Entry type	Down arrow	Up arrow
Numbers only	Sorted from the lowest number to the highest number	Sorted from the highest number to the lowest number
Letters	Sorted left to right, character by character, in alphabetical order.	Sorted left to right, character by character, in reverse alphabetical order.
Alphanumeric	Sorted left to right, character by character, in the following order: from 0 to 9, then in alphabetical order	Sorted left to right, character by character, in the following order: in reverse alphabetical order, then from 9 to 0
Alphanumeric for IP Address fields[(1)]	Addresses are sorted first by type and then alphanumerically from the lowest to the highest number. For example, IPV4, IPV6 and DNS, in the following order: • 2.1.1.1 • 10.2.2.2 • 21.2.1.1 • 21.10.1.1 • 14:C8AA:0:0:0:0:0:EA • 24AA:C8:0:0:0:0:0:EA	Addresses are sorted first by type and then alphanumerically from the highest to the lowest number. For example, DNS address, IPV6, IPV4 in the following order: • 24AA:C8:0:0:0:0:0:EA • 14:C8AA:0:0:0:0:0:EA • 21.10.1.1 • 21.2.1.1 • 10.2.2.2 • 2.1.1.1
Special characters	Sorted left to right, character by character. The following characters are sorted in the following order before numbers, and uppercase and lowercase letters in a list: (space) ! # $ % & ‘ ( ) * + , . / The following characters are sorted in the following order after numbers in a list, but before uppercase and lowercase letters: : ; < = > ? @ The following characters are sorted in the following order after numbers, and uppercase and lowercase letters in a list: { | } ~	Sorted left to right, character by character. The following characters are sorted in the following order before numbers, and uppercase and lowercase letters in a list: ~ } | { The following characters are sorted in the following order before numbers in a list, but after uppercase and lowercase letters: @ ? > = < ; : The following characters are sorted in the following order after numbers, and uppercase and lowercase letters in a list: / . , + *) (‘ & % $ # ! (space)
Blanks	Blank entries are placed first at the top of the list.	Blank entries are placed last at the bottom of the list.

Note

(1) Sorting on an IP Address field may cause performance issues when the 5620 SAM database is under heavy load.

Figure 3-15 List sort order example



Procedure 3-31 To save listed information to a file

After you list information, as described in Procedure 3-30, you can save a copy of the list for purposes such as the following:

- record keeping
- inventory management
- processing by another application

1 Generate a filtered list, as required.

2 Right-click on a list column heading and choose Save To File from the contextual menu. The Save As form opens.

Note — The 5620 SAM uses the user home directory as the default location for saved files.

3 Use the form to specify the name and location of the file that is to contain the listed information. You can save the information in the following formats:

- plain text
- HTML
- CSV

4 Click on the Save button. The information is saved as specified and the Save as form closes.

Procedure 3-32 To save results list preferences

You can save results list preferences, so when similar searches on similar objects are performed, the output of the list is organized according to your preferences.

1 Open a List Form.

2 Organize the results list according to preference, for example, whether to sort columns of data in ascending or descending order.

3 Right-click on a results list column heading and choose Save Table Preferences from the contextual menu. A dialog box appears to confirm that you need to save the current filter preferences.



Note — Choosing Save Table Preferences from a contextual menu does not save any filter configurations.

4 Click on the Yes button. The results list format is saved.

Each time a similar list is generated for similar objects, for example, if you configured a table preference for generating lists of ports, then each time you list ports, results are displayed according to preconfigured table formats.

5 Close the List Form.

Procedure 3-33 To save search filters

List Forms allow you to save filters for object types. The filters created only apply to the specific object type against which the filter is created and saved, and that object type's descendant objects.

1 Open a List Form

2 Define filter properties, as described in Procedure 3-24 and click on the Filter button, or define filter properties, as described in Procedure 3-25. The filter form opens.

3 Click on the Save... button. The Save Filter form opens.

4 Configure the parameters:

- Filter Name
- Description
- Public



Note — These parameters have pre-populated values when a saved search filter is loaded or selected from the saved filters drop-down list, or if the filter was previously saved.

5 Click on the Save button. The Save Filter form closes. The defined filter is saved for a future search on a similar object type and the configured parameters are populated in the filter window.

6 Click on the Apply button of the OK button to use the filter. The results list is displayed based on the filter.

7 If the filter window is open, click on the Close button. The filter window closes.

8 Close the List Form.

Procedure 3-34 To clear a search filter

Use the following procedure to clear search filters from a List Form or the filter window.

1 Open a List Form.

2 Define filter properties as described in Procedure 3-24 or 3-25.

3 Do one of the following.

a To clear all search filters from a List form, go to step 4.

b To clear the search filter of the filter window, go to step 7.

4 Do one of the following.

a Click on the Clear all Filters button. Any filtered properties are cleared.



Note — Clicking on the Clear all Filters button does not clear or refresh search results.

b Choose No Filter from the saved filters drop-down list. Any filtered properties are cleared and the results list is displayed based on the empty filter. Go to step 11.

5 Click on the Search button. The results list is displayed based on the empty filter.

6 Go to step 11.

7 Click on the Filter button. The filter window opens.

8 Click on the Clear button. Any filtered properties are cleared from the filter window.

9 Click on the Apply button or the OK button. The results list is displayed based on the empty filter.

10 If the filter window is open, click on the Close button. The filter window closes.

11 Close the List Form.

Procedure 3-35 To load a saved search filter

Use the following procedure to load search filters from a List Form or the filter window. See Procedure 6-21 for information about loading a saved filter on a topology map.

1 Open a List Form.

2 Do one of the following.

a To load search filters from a List Form, go to step 3.

b To load search filters from the filter window, go to step 4.

3 Choose an entry from the saved filters drop-down list. The results list is displayed based on the filter. Go to step 11.



Note 1 — Choosing an entry from the saved filters drop-down list disables the filter areas of the column headings.

Note 2 — Only saved filters that are applicable to the current object type and its ancestor types appear in the saved filters drop-down list.

Note 3 — Selecting None from the saved filters drop-down list clears any filtered properties on the current form and immediately refresh the results list.

Note 4 — The contents of the filter window are updated based on the entry selected from the saved filters drop-down list.

4 Click on the Filter button. The filter window opens.

5 Click on the Saved Filters button. The Saved Filters window opens and displays filters that have been saved for the current object type and its ancestor type(s).

6 Select a saved filter in the list.

7 Click on the Load button. All the properties of the filter window are replaced with the contents of the saved filter.

8 If desired, modify the filter and click on the Save button to save it.



Note — The filter is saved using the current object type, regardless of the object type of the saved filter that was loaded.

9 Click on the Apply button or the OK button to use the filter. The results list is displayed based on the filter.

10 If the filter window is open, click on the Close button to close the filter window.

11 Close the List Form.

Procedure 3-36 To delete a saved search filter

Use the following procedure to delete saved search filters from the filter window.

1 Open a List Form.

2 Click on the Filter button. The filter window opens.

3 Click on the Saved Filters button. The Saved Filters window opens.

4 Select a saved filter in the list.

5 Click on the Delete button. The filter is deleted.

6 Close the form.

7 Close the filter window.

8 Close the List Form.

Procedure 3-37 To configure equipment group search filters

On some list forms you can create and save search filters based on pre-existing topology groups.

1 Open a list form, if available, choose an entry from the object drop-down list. The equipment group filter drop-down list displays with Equipment Group(s) - All selected.

2 Choose Select Equipment Groups from the equipment group drop-down list. The Select Equipment Groups form appears with the topology groups listed in the Available column. See Procedure 6-28 for information about how to create a topology group.

3 Perform one of the following:

a To create an equipment group filter.

i In the Available list box, choose the topology groups that you need to include in the filter and click on the right arrow. The specified topology groups are moved to the Filtered by list box.

ii To include data from nodes that are in equipment subgroups in the equipment group filter, select the Include contained Equipment Groups check box.

iii Go to step c.

b To modify an equipment group filter.

i Click on the Saved Filters button. The Save Filter form displays the equipment group filters.

ii Select a filter and click on the Load button. The Save Filter form closes and the selected filter is displayed in the Select Equipment Groups form.

iii Update the selected equipment group filter as required.

iv Go to step c.

c To save an equipment group filter.

i Click on the Save button. The Save Equipment Group Filter displays.

ii Configure the parameters:

- Filter Name
- Description
- Public



Note — The parameters have pre-populated values when a saved equipment group filter is loaded or is selected from the saved filters drop-down list, or if the filter was previously saved.

iii Click the Save button. The Save Equipment Group Filter form closes, the filter is saved, and the Select Equipment Groups form displays the saved equipment group filter.

d Click on the Clear button to clear the current filter from the Select Equipment Groups form.

4 Click on the OK button to apply the filter without saving it. The results list is displayed based on the equipment group filter and any additional filters that are applied to the list. The Last Search value is updated, and the equipment group filter name is displayed in the equipment group filter drop-down list.

5 Close the list form.

Procedure 3-38 To perform a search using equipment group filters

On some list forms, you can create and save a filter based on pre-existing topology groups.

1 Open a list form, if available, choose an entry from the object drop-down list. The equipment group filter drop-down list displays with Equipment Group(s) - All selected.

2 Choose a filter from the equipment group drop-down list. The results list is displayed based on the selected equipment group filter and any additional filters that are applied to the list. The Last Search value is updated.

3 Close the list form.

4 — 5620 SAM custom workspaces

4.1 5620 SAM custom workspaces overview *4-2*

4.2 Workflow to administer 5620 SAM custom workspaces *4-3*

4.3 Workflow to customize 5620 SAM workspaces *4-3*

4.4 Workflow to save and update custom workspaces for a 5620 SAM upgrade *4-4*

4.5 5620 SAM GUI custom workspace procedures *4-4*

4.1 5620 SAM custom workspaces overview

Workspace customization

A workspace is the collection of 5620 SAM GUI elements that you use to manage your network. System-defined workspaces are provided, but you can also create and save your own customized workspaces to simplify navigation and operation according to your requirements. You can customize the following workspace elements:

- Menus: You can create custom menus with user-defined names, remove menu items that you don't need, re-order the sequence in which menu items appear, and add grouping separators and custom mnemonics.
- Toolbar: On the toolbar, you can add or remove menu icon buttons, add custom menu drop-downs, create custom toolbar menus, and change the sequence of toolbar items.
- Tree labels: On the routing and equipment navigation trees, you can choose the information to display in the label text fields, and the order in which it appears.
- Topology map icon labels: Map icons can show up to two custom text labels.
- Window layouts: You can save your window layout preferences.

There are three types of workspaces:

- System-defined: These workspaces are read-only and are provided as part of the 5620 SAM product. System-defined workspaces cannot be modified.
- Private: A private workspace contains your customized settings and is visible only to you and an administrator. When you log in to the 5620 SAM, your default custom workspace is displayed.
- Public: A public workspace is usable by all users on the same server.

You can create new custom workspaces based on the system default workspace or on another custom workspace. You must have the required scope of command permissions to create or modify custom workspaces. Scope of command role and user group workspace permissions are set by the system administrator.

The workspace selector located in the upper right-hand corner of the screen contains a list of system default and custom workspaces, and allows you to quickly replace the current workspace with another from this list.You can add or remove custom workspaces in the workspace selector, and change the order in which workspaces appear in the list. See Procedures 4-6 and 4-7.

5620 SAM upgrades and custom workspace updates

New releases of the 5620 SAM may contain newly-introduced menu items. You can add these new menu items to the custom workspaces of an earlier release. You can export custom workspaces to a specified directory, and import them later into an upgraded version of the 5620 SAM. After an upgrade, the 5620 SAM lists all newly-introduced menu items, which you can add to the imported workspace as required. See Procedure 4-11.

Custom tab display

You can also customize the display of tabs on configuration forms, and save your tab display preferences. For specific forms, you can display, hide, or arrange the sequence of tabs according to your operational requirements. See Procedure 3-20.

Custom settings for tabs on configuration forms are saved as user preferences. They are not affected by a change of workspaces.

4.2 Workflow to administer 5620 SAM custom workspaces

A system administrator performs the following tasks to configure users and permissions for custom workspaces:

1. Configure the scope of command roles for workspaces; see the *5620 SAM System Administrator Guide*.
2. Add or delete workspaces in a User Group, as required; see the *5620 SAM System Administrator Guide*.

4.3 Workflow to customize 5620 SAM workspaces

1. Assess your operational requirements to determine your workspace element needs.
2. Create a custom workspace; see Procedure 4-1.
3. Customize menus; see Procedure 4-1.
4. Customize toolbars; see Procedure 4-2.
5. Customize tree labels; see Procedure 4-3.
6. Customize topology map icon labels; see Procedure 4-4.
7. Customize window layouts; see Procedure 4-5.
8. Add or remove custom workspaces and arrange their sequence in the workspace selector; see Procedure 4-6.
9. Delete a workspace when it is no longer required; see Procedure 4-8.



Note — You can also customize the display of tabs on configuration forms, and save your tab display preferences. For specific forms, you can display, hide, or arrange the sequence of tabs according to your operational requirements. See Procedures 3-20 and 3-21.

4.4 Workflow to save and update custom workspaces for a 5620 SAM upgrade

1. Export custom workspaces to a specified directory; see Procedure 4-9.
2. Perform an upgrade on the 5620 SAM.
3. Import workspaces from a directory into the 5620 SAM; see Procedure 4-10.
4. Update the custom workspace of an earlier 5620 SAM release with a new menu item from a later release; see Procedure 4-11.

4.5 5620 SAM GUI custom workspace procedures

The following procedures describe how to create and manage custom workspaces in the 5620 SAM.

Procedure 4-1 To customize menus

Perform this procedure to customize menus in a new workspace or to modify menus in an existing workspace.

You must have the required scope of command permissions to customize workspaces.

1 Open the Workspace form. Perform one of the following:

a Create a new workspace based on the system default workspace:

i Choose Application→Manage Workspaces from the 5620 SAM main menu. The Manage Workspaces form opens.

ii Click on the Create button. The Workspace (Create) form opens.

iii Configure the parameters:

- Name
- Description
- Scope



Note — Based on your assigned scope of command role and permissions, you can configure the scope. Otherwise, Private will be set by default and cannot be modified.

b Create a new workspace based on an existing custom workspace:

i Choose Application→Manage Workspaces from the 5620 SAM main menu. The Manage Workspaces form opens.

ii Choose a custom workspace in the list as the basis for the new workspace and click on the properties button. The Workspace (Edit) form opens.

iii Click on the Copy button.

iv Configure the parameters:

- Name
- Description
- Scope



Note — Based on your assigned scope of command role and permissions, you can configure the scope. Otherwise, Private will be set by default and cannot be modified.

c Modify an existing custom workspace:

i In the workspace selector, select the custom workspace you need to modify.

ii Choose Application→Customize Current Workspace from the 5620 SAM main menu.

Alternatively, you can select a custom workspace from the list on the Manage Workspaces form and click on the Properties button.

The Workspace (Edit) form opens.



Note 1 — You cannot modify a system default workspace using the Customize Current Workspace option.

Note 2 — You must have the required scope of command to customize an existing workspace.

2 Click on the Menus tab.

The All Menu Items panel contains a list of all available menu items in the 5620 SAM. The Custom Menu panel contains a list of all menu items in the custom workspace.

3 Expand items as required in the All Menu Items panel and Custom Menu panel.

4 In the Custom Menu panel, remove any menu items that are not required in the workspace. To remove, select the items and delete using the right-click menu or the keyboard.

Consider the implications of removing menu items from your workspace. For example, do not delete the User Preferences or Manage Workspaces menu items. These items are required for later custom workspace configuration and access to other workspaces.

5 Add menu items to the Custom Menu panel as required. Select items in the All Menu Items panel. You can click and drag, right click, or use the keyboard to copy selected menu items to the Custom Menu panel.

The orange check box beside an item in the All Menu Items panel indicates whether the sub-menu items for that menu item are all used, partially used, or not used in the Custom Menu. Check box symbols are described in the Legend at the bottom of the Workspace form. The check boxes reduce the need to compare sub-menus between the All Menu Items panel and the Custom Menu panel.

6 Move items in the Custom Menu panel as required. You can click and drag items, or use right click or the keyboard to cut, copy and paste selected menu items to other locations in the Custom Menu panel.

If you hold the CTRL key while dragging, the drop action changes from move to copy.

7 Rename items in the Custom Menu panel as required. Select the item, right-click and choose Rename, then type a name and press Enter.

Modified menu items are displayed in blue.

8 Add grouping separators in sub-menus, as required. Right click in the location where you need to add a separator and choose Add Separator.

9 Edit the mnemonic for an item in the Custom Menu panel. Perform the following:

i Select the item, right-click, and choose Edit Mnemonic. A drop-down opens.

ii Choose a letter from the drop-down and click OK.

The mnemonic letter is underlined in the menu item name and is used with the CTRL key as a keyboard shortcut. The mnemonic for each item in a sub-menu must be unique.

10 Add a new custom menu in the Custom Menu panel. Select an item, right-click, and choose Add Menu. A new menu item appears under the selected item. Type a name for the new item and press Enter.

If you right-click on empty space in the panel, the new menu item appears as the last item in the list.

You can use new menus to contain custom menus for functions you use often.

11 To locate a sub-menu item in the Custom Menu panel, you can display the menu path for the item. Perform the following:

i In the All Menu Items panel, select an item, right-click, and choose Show in Custom Menu Tree.

A dialog box displays the path for the item in the Custom Menu. If the item appears more than once in the Custom Menu tree, multiple paths are displayed.

ii Click on the OK button to close the dialog box.

12 To locate a sub-menu item in the All Menu Items panel, you can display the menu path for the item. Perform the following:

i In the Custom Menu panel, select an item, right-click, and choose Show in All Menu Items Tree.

A dialog box displays the path for the item in the All Menu Items panel.

ii Click on the OK button to close the dialog box.

13 Click on the OK button. A dialog box is displayed.

14 Click on the Yes button. The Workspace form closes.



Note — When you modify the current workspace, the workspace selector displays Workspace Out of Sync. Select the current workspace from the workspace selector drop-down to update to the modified settings.

Procedure 4-2 To customize toolbars

The 5620 SAM toolbar contains icon buttons that allow quick access to menu items. Custom toolbars can also contain drop-down menus. Perform this procedure to add or remove buttons and menus, and to change the order of buttons and menus on the toolbar.

1 Open the Workspace form as described in step 1 of Procedure 4-1.

2 Click on the Toolbar tab.

The Custom Menu panel contains a list of all the menu items in the custom workspace. The Appear on Toolbar panel displays a list of all items displayed as buttons or menus on the toolbar.

3 Expand items as required in the Custom Menu panel and Appear on Toolbar panel.

4 In the Appear on Toolbar panel, remove any items that are not required on the toolbar. To remove, select the items and use the right-click menu or the keyboard to delete.

5 Add menu items to the Appear on Toolbar panel as required. Select items in the Custom Menu panel. You can click and drag, right click, or use the keyboard to copy selected items to the Appear on Toolbar panel.

When you add a menu item that contains a sub-menu, a drop-down for the item is added to the toolbar. When you click on the drop-down on the toolbar, the sub-menu items are displayed. Menu items that contain sub-menus are displayed with a folder icon in the Workspace panels.

When you add an item with no sub-menu, the item appears on the toolbar as an icon button. Menu items with no sub-menus are displayed with unique identifying icons.

Menu items without icons can only be pasted in a menu folder. For example, menu items in the Window menu do not display icons.

The orange check box beside an item in the Custom Menu panel indicates whether the sub-menu items for that menu item are all used, partially used, or not used in the custom toolbar. Check box symbols are described in the Legend at the bottom of the Workspace form.

6 Move items in the Appear on Toolbar panel as required. You can click and drag items, or use right click or the keyboard to cut, copy and paste selected menu items to other locations in the Appear on Toolbar panel.

If you hold the CTRL key while dragging, the drop action changes from move to copy.

7 Rename items in the Appear on Toolbar panel as required. Select the item, right-click and choose Rename, then type a name and press Enter.

Modified menu items are displayed in blue.

8 Add a custom menu item in the Appear on Toolbar panel. Select an item, right-click, and choose Add Menu. A new menu item appears under the selected item. Type a name for the new item and press Enter.

If you right-click on empty space in the panel, the new menu item appears as the last item in the list.

You can use new menus to contain custom menus for functions you use often.

9 To locate a sub-menu item in the Custom Menu panel, you can display the menu path for the item. Perform the following:

i In the Appear on Toolbar panel, select an item, right-click, and choose Show in Custom Menu Tree.

A dialog box displays the path for the item in the Custom Menu. If the item appears more than once in the Custom Menu tree, multiple paths are displayed.

ii Click on the OK button to close the dialog box.

10 Click on the OK button. A dialog box is displayed.

11 Click on the Yes button. The Workspace form closes.



Note — When you modify the current workspace, the workspace selector displays Workspace Out of Sync. Select the current workspace from the workspace selector drop-down to update to the modified settings.

Procedure 4-3 To customize tree labels

In the 5620 SAM GUI, objects in the Equipment and Routing navigation trees are displayed with icons and labels. Labels are displayed as text fields separated by commas. Each label type corresponds to specific information. For example, the Software Version label type displays in the text field as the release number of the NE.

You can customize the display of text labels for tree objects by selecting the label types that appear and the order in which they appear. You can select and order up to two label types for objects at the top level of the tree, and up to five label types at the NE level. Labels for the Unmanaged NEs, Discovered NEs or Network Groups objects cannot be customized.

Perform this procedure to customize the labels for Equipment and Routing navigation tree objects.

1 Open the Workspace form as described in step 1 of Procedure 4-1.

2 Click on the Tree tab and choose the tree type from the drop-down menu.

3 Object types and text fields are displayed in a table. In the Equipment Group (All) table row, perform the following:

   i Click on the table cell below Text Field #1 and choose a label type from the drop down menu.The selected label type appears in the table cell. On the navigation tree, specific information for the label type will appear in the Text Field #1 position for the object.

   ii Click on the table cell below Text Field #2 and choose a label type from the drop down menu.The selected label type appears in the table cell.

4 Continue for the remaining rows in the table, as required. For Network Element rows, you can configure up to five text fields. Some label types appear below more than one text field heading. You can specify the display sequence of these labels by choosing which text field to display them in.



Note 1 — Click on Restore Defaults to reset text fields to the default values for the tree type in view.

Note 2 — The label types for each object are displayed in navigation tree tooltips.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Workspace form closes.



Note — When you modify the current workspace, the workspace selector displays Workspace Out of Sync. Select the current workspace from the workspace selector drop-down to update to the modified settings.

7 Close the Manage Workspaces form.

Procedure 4-4 To customize topology map icon labels

By default, topology map icons include a descriptive label. For example, the label on a managed device icon on the service topology map includes the service name and the IP address of the device.

Perform this procedure to customize labels for topology map icons.

1 Open the Workspace form as described in step 1 of Procedure 4-1.

2 Click on the Topology tab. A list of topology map icons is displayed in a table.

3 Select a topology map icon. The table row is highlighted.

4 Click in the highlighted row below Text Field #1 and Text Field #2 to select the information to display for the map icon label.

5 Repeat steps 3 and 4 to customize additional icon labels.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button to save the changes and close the dialog box.

8 Close the Manage Workspaces form.



Note — When you modify the current workspace, the workspace selector displays Workspace Out of Sync. Select the current workspace from the workspace selector drop-down to update to the modified settings.

Procedure 4-5 To customize window layouts

Perform this procedure to select the window layout that appears when the 5620 SAM opens. You can select the system default or the current window layout. See Procedure 3-9 for information about how to arrange windows in the 5620 SAM GUI.

1 Open the Workspace form as described in step 1 of Procedure 4-1.

2 Click on the Window Layout tab.

3 Set the Window Layout to specify the window layout when the 5620 SAM opens. Select one of the following:

- Default (Default)—The navigation tree, Alarm Window, topology map and the main GUI client will open at the system default size and location
- Set to Current (Custom)—The navigation tree, Alarm Window, topology map, and the main GUI client will open at the currently displayed size and location

4 Click on the OK button. A dialog box appears.

5 Click on the Yes button and close the Manage Workspaces form.



Note — When you modify the current workspace, the workspace selector displays Workspace Out of Sync. Select the current workspace from the workspace selector drop-down to update to the modified settings.

Procedure 4-6 To add or remove a workspace in the workspace selector

Perform this procedure to add or remove custom workspaces or change the sequence of workspaces in the workspace selector, or to set a custom workspace as the default workspace.

1 Choose Application→User Preferences from the 5620 SAM main menu. The User Preferences form opens.

2 Click on the Workspaces tab. A list is displayed of the workspaces that are currently listed in the workspace selector.

3 Add a workspace to the workspace selector. Perform the following:

- **i** Click on the Add button. The Add Workspace form opens. A list is displayed of the workspaces not currently in the workspace selector.
- **ii** Choose a workspace from the list.
- **iii** Click on the OK button. The Add Workspace form closes and the workspace is displayed in the list on the Workspaces tab of the User Preferences form.

4 Set the default workspace that displays when the 5620 SAM opens. Choose the workspace in the list and click on the Set as Default button.

5 Remove a workspace from the workspace selector. Choose a workspace in the list on the Workspaces tab and click on the Delete button.



Note 1 — You cannot remove the System_Default_All workspace from the workspace selector.

Note 2 — If a user has the deleted workspace as the default workspace, their new default workspace is System_Default_All and the workspace selector displays “Workspace Out of Sync”.

6 Change the sequence of workspaces in the workspace selector. Choose a workspace in the list on the Workspaces tab and click on the Move Up or Move Down buttons.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The User Preferences form closes. The workspace selector drop-down in the top right corner of the menu bar is updated with the new settings.

Procedure 4-7 To change to another workspace using the workspace selector



Note — You must add a custom workspace to the workspace selector before you can select it. See Procedure 4-6.

1 Click on the workspace selector drop-down in the top right corner of the display.

2 Choose a workspace in the list. The 5620 SAM GUI is displayed using the settings from the selected workspace. The workspace selector displays the workspace currently in use.

Procedure 4-8 To delete a workspace from the 5620 SAM

Perform this procedure to permanently delete a custom workspace from the 5620 SAM. You must have the required scope of command permissions to delete a custom workspace. System default workspaces cannot be deleted.

1 Choose Application→Manage Workspaces from the 5620 SAM main menu. The Manage Workspaces form opens.

2 Choose a workspace in the list and click on the Delete button. A dialog box opens.

3 Click on the Yes button to confirm the action.

4 Close the Manage Workspaces form.



Note 1 — When you delete the current workspace, the workspace selector displays “Workspace Out of Sync”. Select another workspace in the workspace selector.

Note 2 — If a user is deleted from 5620 SAM, the private workspaces of the user are deleted from the database.

Procedure 4-9 To export custom workspaces

You can save custom workspaces by exporting them, and then import them later into upgraded versions of the 5620 SAM. Perform this procedure to export workspaces, based on your scope of command permissions.

1 Choose Application→Manage Workspaces from the 5620 SAM main menu. The Manage Workspaces form opens.

2 Perform one of the following:

a To export all custom workspaces, click on the Export All button. The Export Directory window opens.

If you have workspace permissions enabled, all public and private workspaces can be exported. If you have workspace permissions disabled, only private workspaces can be exported.

b To export selected multiple workspaces, choose the custom workspaces in the list and click on the Export button. The Export Directory window opens.

c To export a single custom workspace, choose the workspace in the list and click on the Export button. The Export Directory window opens.

Alternatively, you can click on the Properties button for a selected custom workspace to open the Workspace (Edit) form, then click on the Export button.



Note — If you do not have permissions to export a workspace the Export button is disabled.

3 Specify the export directory in the Save In drop-down menu or create a directory or folder. A warning is displayed.

4 Click on the Yes button to create or overwrite the directory. The selected workspace files are exported to the specified directory on the server.

Procedure 4-10 To import a workspace

Perform this procedure to import 5620 SAM workspaces that were previously saved as exported workspaces. For information about how to export workspaces, see Procedure 4-9.

1 Choose Application→Manage Workspaces from the 5620 SAM main menu. The Manage Workspaces form opens.

2 Click on the Import button to import previously exported workspaces. The Import Directory window opens.

3 Use the Look In drop-down menu to choose the directory from which to import a workspace.



Note — If you need to overwrite the user name or overwrite existing workspaces, select either the Overwrite User Name or the Overwrite Existing Workspace(s) check box. Based on your user permissions, some of the options may not be configurable.

4 Click on the Open button. The imported workspaces are added to the Manage Workspaces form.



Note — You cannot import the same workspace multiple times. A warning message is displayed.

Procedure 4-11 To add new menu items to a saved custom workspace after a 5620 SAM upgrade

When you upgrade to a later release of the 5620 SAM, you can update your custom workspaces of an earlier release by adding menu items that are new in the later release. You can view the new menu items and add them to custom workspaces imported from an earlier release.

After an upgrade, the workspace is auto-created from an existing saved GUI preference file if it exists on the local file system, with a *username_hostname* workspace name. If this name exists, the workspace name will be *username_hostname_timestamp*. When you log in to the client after an upgrade, the custom workspace is displayed.

Perform this procedure to add new menu items to an existing custom workspace of an earlier release.



Note 1 — You must have the required scope of command role and permissions to view or add new menu items.

Note 2 — The New Menu Items function is available after an upgrade to the 5620 SAM.

1 Choose Application→Manage Workspaces from the 5620 SAM main menu. The Manage Workspaces form opens.

2 Choose one of the following:

- **a** Import a saved workspace from an earlier 5620 SAM release. See Procedure 4-10.
- **b** After an upgrade, when you log in as an existing user, select a custom workspace from an earlier 5620 SAM release.

3 Click on the Properties button. The Workspace (Edit) form opens. The All Menu Items option is displayed by default.

4 Configure the parameters, if required:

- Name
- Description
- Scope

5 From the All Menu Items drop-down menu, choose New Menu Items. A list of menu items newly-introduced in the 5620 SAM since the earlier release is displayed.

6 Add menu items to the Custom Menu panel as required. See Procedure 4-1.

7 Select the Finished adding New Menu Items check box to update the workspace.



Note — After the Finished adding New Menu Items check box is selected and you click on the Apply or OK buttons, the New Menu Items drop-down is no longer displayed and you can no longer view the New Menu Items list.

8 Click on the Apply or OK button. A dialog box appears.

9 Click on the Yes button and close the Workspace (Edit) form.

5 — 5620 SAM navigation tree overview

5.1 Navigation tree overview *5-2*

5.2 Basic navigation tree procedures *5-11*

5.1 Navigation tree overview

The navigation tree lists the managed equipment, services, and protocols that are configured on the NE. The navigation tree includes a view selector located on the navigation tree toolbar. The view selector is a drop-down menu that lists the physical and logical network views that are available.

The navigation tree is accessible from the main window, configuration forms, and maps.

You can choose the following views:

- Equipment—displays the physical objects that the 5620 SAM manages
- OSPF—displays the OSPF objects in the network
- IS-IS—displays the IS-IS objects in the network
- Routing—displays the device routing instances and child objects such as the network interfaces and the configured protocols
- Ring Group—displays the ring group objects that the 5620 SAM manages

You can use the navigation tree to search for specific objects such as NEs, shelves, cards, and ports in the physical and logical network views. See Procedure 5-1 for information about searching for objects using the navigation tree.

Table 5-1 describes the objects in the equipment view of the navigation tree that the 5620 SAM allows you to create and manage.



Note — The device properties forms include a navigation tree that is displayed on the left of the form. The root of the device properties form navigation tree is the device.

Table 5-1 5620 SAM navigation tree object descriptions — Equipment view

Object	Description
Routing	The network — contains the routers, devices, and topology groups, including the default Discovered NEs and Unmanaged NEs topology groups
NE, topology group	The second level in the hierarchy
CCAG, ISA-AA groups, ISA-Tunnel groups, ISA-LNS groups, ISA-NAT groups, ISA-Video groups, LAG, IGH, shelf	The third level in the hierarchy
APS groups	Located under the shelf object; contain the APS groups for a device
Card	Located under the shelf object
Daughter card	A child object of the card object
Bundles	A child object of the daughter-card object; a group of DS0 channels on a SONET- or TDM-capable daughter card
Port	A child object of the daughter-card object

(1 of 2)

Object	Description
Channel, sub-channel, timeslot	Child objects of the port object
Fans	Located under the shelf object(1)
Power Supplies	Located under the shelf object(1)

(2 of 2)

Note
(1) This object is not supported on 1830 PSS nodes.

You can use the following methods to view and manage objects in the 5620 SAM navigation tree:

- Double-click on an object or press the + key when the object is selected to open the object and to display the child objects.
- Double-click on an object or press the - key when the object is selected to close the object and to hide the child objects. A + key to the left of the map object indicates that the object contains child objects. For example, a topology group that contains one or more child topology groups has a + key to the left of the topology group in the navigation tree.
- Click on an object and use the cursor keys to navigate the object hierarchy. In the Equipment view, for example, you can navigate from the device to the ports and channels.
- Right-click on an object to open the contextual menu and choose a function. The menu options are specific to the object type. See "Contextual menus" in this section for more information.



Note — Keyboard-based navigation-tree operations may not function as expected when you open the client GUI using a third-party access tool, for example, a Citrix server.

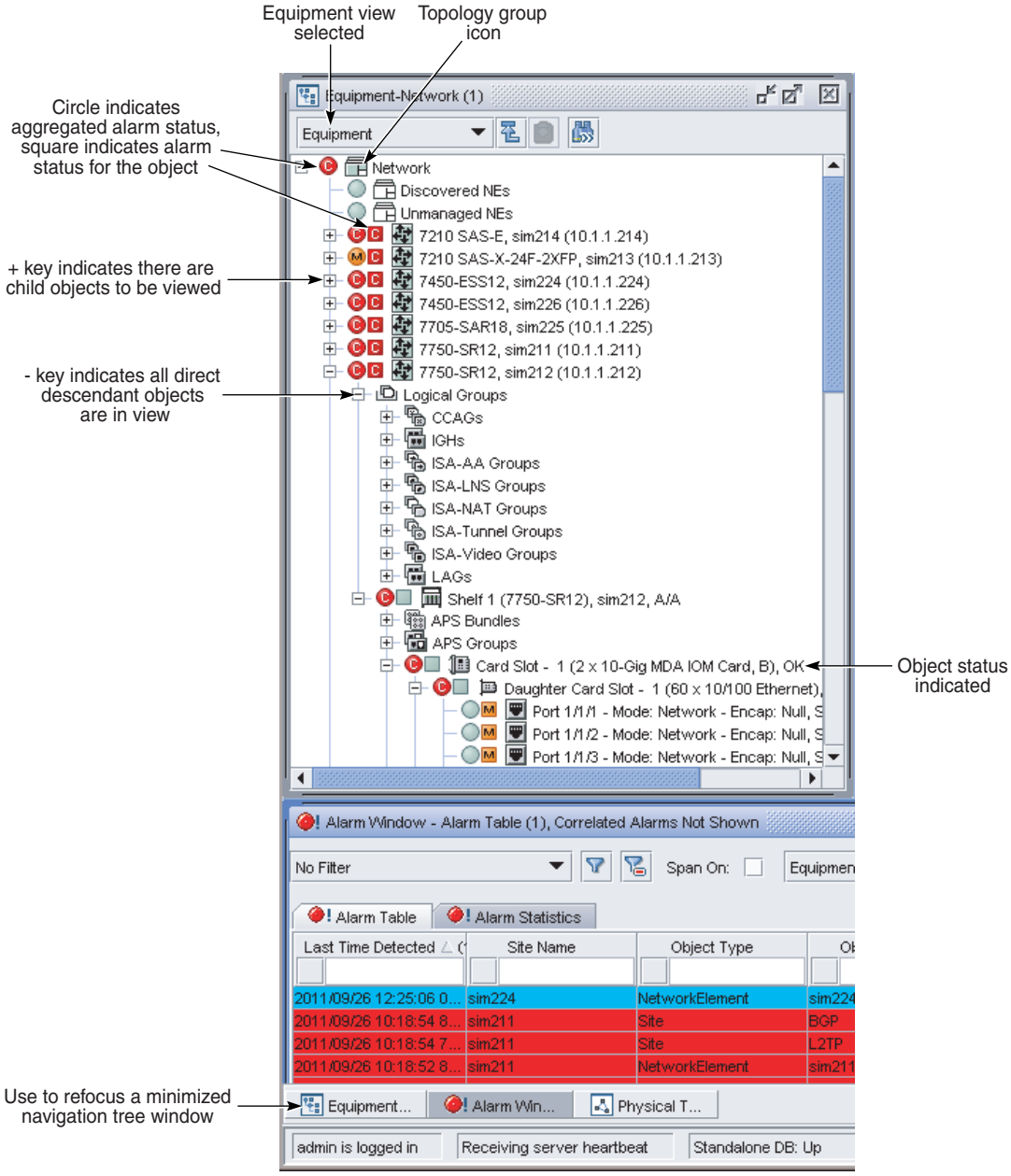
The navigation tree uses color highlights to display object status information such as the current alarm level and the aggregated alarm status. The operational and administrative states of an object are displayed in text form beside the object icon, as are the object type and description.

The circle icon to the left of the topology group icon represents the aggregated alarm status for the group. It represents the most serious alarm against descendant device.

The topology group icon is divided into three sections. The top right square represents the most severe state of all descendant devices. The bottom right square represents the most severe state of all descendant links. The bottom section of the topology group icon represents the most severe state of the devices and edges that are immediately descendant of the group. See chapter 31 for more information about viewing alarm status information in a map navigation tree. To troubleshoot alarms using topology maps, see *5620 SAM Troubleshooting Guide*.

Figure 5-1 shows some of the navigation tree objects that you can manage using the Equipment view.

Figure 5-1 5620 SAM navigation tree objects - Equipment view



18030

Using the navigation tree toolbar

The navigation tree toolbar consists of the view selector, the Make Root At Top Level button, and the Copy to Clipboard button. Figure 3-1 shows the navigation tree toolbar. See Procedure 3-15 for information about using the Copy to Clipboard button.

Make Root At Top Level button

The Make Root At Top Level button restores the navigation tree to the default root. For example, in the equipment view, if you redefine the root of the tree as a card and click on the Make Root At Top Level button, the navigation tree refreshes with the default root, which is the network. The Make Root At Top Level button is enabled only when the root is not the network. The Make Root At Top Level button is available only for the equipment view.

Make Root and Make Root In New Tree menu options

The navigation tree contextual menus provide Make Root and Make Root In New Tree menu options that allow you to redefine the root of the tree. These menu options, along with the Make Root At Top Level button, help orient users in densely populated navigation trees. The menu options are available only for the equipment view. See "Contextual menus" in this section for more information about using these functions.

Copy to Clipboard button and Clipboard window

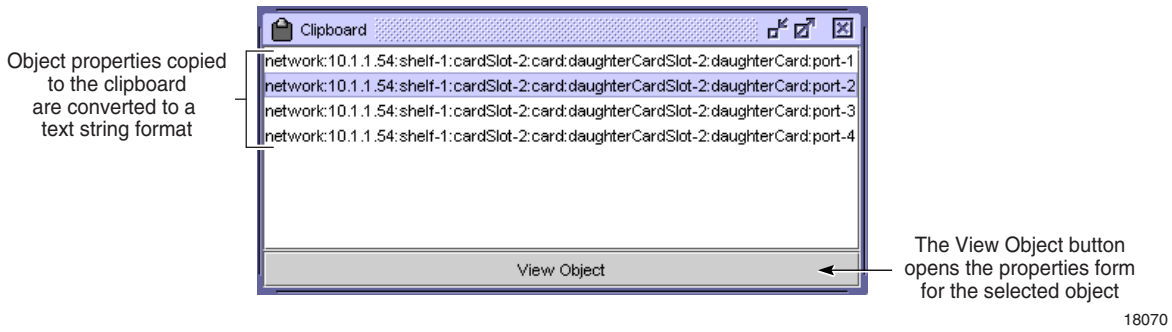
Using the Copy to Clipboard button on the navigation tree toolbar, you can copy the identifier of one or more 5620 SAM objects to the Clipboard window. You can then open the Clipboard window from the Application menu to retrieve the identifier and paste it into another application. You can also choose an object identifier in the Clipboard window and click on the View Object button to open the object properties form. The elements in an object identifier are delimited using colons (:).

The Copy to Clipboard button is on list forms and on the list tabs of properties forms. You can use the button to copy configurable and read-only text fields. The button is enabled when at least one object is selected.

Note — The Clipboard window keeps the object identifier from only the most recent copy action. After you copy an object identifier to the clipboard, if you click on the Copy to Clipboard button again to copy another object identifier, the second copy action overwrites the previously copied identifier in the Clipboard window.

Figure 5-2 shows the Clipboard window. See Procedure 3-15 for more information about using the clipboard function.

Figure 5-2 Clipboard window



Paste from Clipboard button

After using the Copy to Clipboard button to copy object identifiers to the Clipboard window, you can use the Paste from Clipboard button on the physical link properties form to set multiple parameters at one time using the copied object identifiers. See Procedure 6-33 for information about using the Paste from Clipboard button.

Contextual menus

Each object in the 5620 SAM navigation tree has a contextual menu that opens when you right-click on the object. Contextual menus are also accessible when you right-click on map objects.

You can use the contextual menus to do the following:

- create objects
- configure object properties
- perform maintenance functions
- change the state of objects
- open a different management interface, for example, a CLI
- designate an object as the root object in the navigation tree

The contextual menu options are specific to the object type. Table 5-2 lists the contextual menu options in alphabetical order.

Table 5-2 Contextual menu options

Option name	Description
Add to Ring Group	The Add to Ring Group menu option specifies whether to add the device to a group.
Alternate Element Manager	The Alternate Element Manager option opens an alternate EMS client on the 5620 SAM client station. The option is available for GNEs only, and only when the EMS client application is specified in the GNE configuration or in the associated GNE profile.
Configure Card	The Configure Card option opens the Create Card properties form that allows you to create a card configuration for the slot. You assign a supported card type to the slot. The options available are displayed with check marks beside them in the Supported Card Types parameter. The Equipped Card Type displays the card type that is physically in the slot. When the configured card types are correct, you can change the Administrative State as required.
Configure Daughter Card	The Configure Daughter Card option opens the Daughter Card (Create) form that allows you to create a daughter card configuration for the slot. You assign a supported daughter card type to the daughter card slot. The options are displayed with check marks beside them in the Supported Daughter Card Types area of the form. The Equipped Daughter Card Type displays the daughter card type that is physically in the slot. When the configured card types are correct, you can change the Administrative State as required.
Copy to Clipboard	The Copy to Clipboard option copies the MDA information to the clipboard.

(1 of 6)

Option name	Description
Create APS Group	The Create APS Group menu option opens the APS Group (Create) form that allows you to create and manage SC APS groups and MC APS groups on the shelf.
Create APS Protection Bundle	The Create APS Protection Bundle menu option opens the Create Multilink Bundle form, which allows you to create and manage APS protection bundles. You must create an APS working bundle before you can create an APS protection bundle or add members to the APS bundle.
Create APS Protection Channel	The Create APS Protection Channel menu option opens the APS Channel, Protection (Create) form that allows you to create and manage APS protection channels.
Create APS SONET Channel	The Create APS SONET Channel menu option opens the SONET Channel (Create) form that allows you to create the APS common configuration.
Create APS Working Bundle	The Create APS Working Bundle menu option opens the Create Multilink Bundle form, which allows you to create and manage APS working bundles. You must create an APS working bundle before you can create an APS protection bundle or add members to the APS bundle.
Create APS Working Channel	The Create APS Working Channel menu option opens the APS Channel, Working (Create) form that allows you to create and manage APS working channels.
Create Bundle Members	The Create Bundle Members option opens the Add Bundle Member form, which allows you to add members to an APS bundle or a multilink bundle.
Create Bundle	The Create Bundle option opens the APS Bundle Display configuration form or the Create Multilink Bundle configuration form, which allows you to create a group of DS0 channel groups on a channelization-capable MDA. You configure bundle parameters and add bundle members. When the Create Bundle option is used to open the APS Bundle Display configuration form, the DS0 channel groups that you create provide bidirectional APS protection on IMA bundles. When the Create Bundle option is used to open the Create Multilink Bundle configuration form, the DS0 channel groups that you create provide a mechanism to distribute data across multiple links to achieve higher bandwidth on a SAP. You can create IMA group bundles on channelized ASAP MDAs.
Create CCAG	The Create CCAG option opens the CCAG (Create) form, which allows you to create a cross-connect aggregation group. You define CCAG properties, configure CCAG parameters, and configure CCAG members.
Create Channel	The Create Channel option allows you to create channels on ports with available channels.
Create Group	The Create Group contextual menu option opens the Group (Create) form to create a topology group in the equipment view of the navigation tree and on the appropriate topology maps.
Create IGH Members	The Create IGH Members option opens the Create IGH Member configuration form which allows you to configure IGH member ports.
Create IGH	The Create IGH option opens the IGH (Create) form, which allows you to create an IGH. You define IGH properties, and configure IGH subgroups and members.

(2 of 6)

Option name	Description
Create ISA-AA Group	The Create ISA-AA Group option opens the ISA-AA Group (Create) form, which allows you to create an ISA-AA group and ISA-AA partitions. You define ISA-AA group and ISA-AA partition properties, configure ISA-AA group and ISA-AA partition parameters, and specify ISA-AA members.
Create ISA-Tunnel Group	The Create ISA-Tunnel Group option opens the ISA-Tunnel Group (Create) form, which allows you to create an ISA-Tunnel group. You define ISA-IPsec properties, configure ISA-IPsec parameters, and specify ISA-IPsec members.
Create ISA-LNS Group	The Create ISA-LNS Group option opens the ISA-LNS Group (Create) form, which allows you to create an ISA-LNS group. You define ISA-LNS properties, configure ISA-LNS parameters, and specify ISA-LNS group members.
Create ISA-NAT Group	The Create ISA-NAT Group option opens the ISA-NAT Group (Create) form, which allows you to create an ISA-NAT group. You define ISA-NAT properties, configure ISA-NAT parameters, and specify ISA-NAT group members.
Create ISA-Video Group	The Create ISA-Video Group option opens the ISA Video Group (Create) form, which allows you to create an ISA-Video group. You define ISA-Video properties, configure ISA-Video parameters, and specify ISA-Video group members.
Create LAG Members	The Create LAG Members option opens the Create LAG Member configuration form where you define LAG member ports.
Create LAG	The Create LAG option opens the Create LAG configuration form. You define LAG properties, configure LAG parameters, configure LAG subgroups and members, and configure LACP.
Create Maximum # of Channels	The Create Maximum # of Channels option allows you to automatically create all of the channels on ports with available channels. This option is available for OC3, OC12, DS3 ASAP, E3 ASAP, APS Common ports, and APS SONET VTG ports.
Create Ring Group	The contextual menu option for a network is Create Ring Group, which is used to group devices to be able to create VLAN or VPLS ring groups.
Delete	For daughter cards, bundles, ports, and channels, the Delete option deletes the selected object when the object and everything contained in the object is set to administratively down. For topology groups, and IGH groups, the Delete option deletes the selected group object once all objects in the group have been removed from the group. For SC APS Bundle objects, the Delete option deletes the APS common configuration from the APS group. For all other objects where the Delete option is available, the Delete option deletes the object and all contained objects from the network. This option is not available for the network (root) topology group.
Discovery Manager	On the physical topology map background, the Discovery Manager option opens the Discovery Manager (Edit) form. You can create NE discovery rules and discover NEs. See chapter 10 for information about discovering NEs and creating discovery rules.

(3 of 6)

Option name	Description
Duplicate Links	On the physical topology map background, the Duplicate Links option displays a drop-down menu. You can choose either the Highlight Duplicate Links or Delete Duplicate Links option. It is possible for both a manual link and a discovered physical link to exist on the same two endpoints. When this happens, a duplicate link alarm is raised. This alarm only occurs on point-to-point links and when both endpoints are ports or LAGS. You can identify such duplicate links by choosing the Highlight Duplicate Links option. You can remove these duplicate links by choosing the Delete Duplicate Links option. This action prompts you with a warning and then delete all of the manually created physical links. This alarm is not raised on existing manual links (for example, those in place after a database upgrade).
Equipment	On the physical topology map background, the Equipment option opens a Group (Create) form to create a descendant topology group for the selected group in the navigation tree. For physical topology maps, you can also choose the Create Physical Link option to create links between map objects.
Force Mode	The Force Mode menu option forces an upgrade of the hardware.
Highlight MTU Mismatch	On the physical topology map background, the Highlight MTU Mismatch option is used to highlight MTU mismatches between physical ports. When the configured MTU on two or more endpoints do not match, an alarm is raised to notify the operator of a possible configuration error. This is supported on both point-to-point and broadcast physical links. MTU mismatches can also be discovered by conducting an RCA audit. See Procedure 80-6 for more information.
Highlight Nearest Customer Links	On the physical topology map background, the Highlight Nearest Customer Links option is used to highlight the nearest customer links between nodes. See "LLDP" in chapter 22 for more information.
Highlight Nearest Non-TPMR Links	On the physical topology map background, the Highlight Nearest Non-TPMR Links option is used to highlight the nearest Non-Two Port MAC Relay links between nodes. See "LLDP" in chapter 22 for more information.
Highlight Upper Layer Adjacency Links	On the physical topology map background, the Highlight Upper Layer Adjacency Links option is used to display hidden links between nodes.
List	From the contextual menu for the default Discovered NEs topology group, the List option opens the Discovered NEs form with a list of newly discovered NEs or the Unmanaged NEs form with a list of newly added Unmanaged NEs.
Make Flat Map for Group	The Make Flat Map for Group option opens a flat map of the topology group.
Make Root	The Make Root option makes the selected object the root of the navigation tree. The default root is the network.
Make Root In New Tree	The Make Root In New Tree option opens another navigation tree window with the selected object as the root of the tree.
NE Sessions	The NE Sessions option opens a Telnet session, an SSH session, an FTP file browser session, or an SSH file browser session with the selected device in the equipment view of the navigation tree.
Open URL	The Open URL option opens the Web browser to manage the GNE.

(4 of 6)

Option name	Description
Properties	The Properties option opens the property form for the selected object. This form allows you to view read-only information and to configure parameters associated with the selected object. If the Copy button is available, you can use the Copy button to create topology groups in the network using the same parameter information.
Reboot	The Reboot option specifies that the selected card in the chassis is re-initialized. For the 7705 SAR-M, if the Reboot option is issued from Daughter Card Slot 1, then all daughter cards will be rebooted. However, if the Reboot option is issued from Daughter Card Slot 3, then only that daughter card will be rebooted. The Reboot option is not available if Daughter Card Slot 2 is selected.
Reference	On the physical topology map background, the Reference option takes a snapshot of the physical topology at a specific time. Any deviation from this checkpoint can then be subsequently shown. You can choose from the following options: • Reference all Discovered Links in NE Group - checkpoints all currently discovered links that exist. Any object that was previously checkpointed and is operationally down is left untouched. Any object that goes operationally down in the future is not removed, but is simply marked as operationally down. • Clear Reference for All Discovered Links in NE Group - clears all object checkpoints. Any object that is operationally down (shown as a red link) is removed from the database. Any non-checkpointed object that becomes operationally down in the future is removed from the system. • Cleanup all Discovered Links in NE Group - keeps the current checkpoint set for objects that are operationally up, but removes checkpoints from objects that are operationally down. This is the same as the Clear Reference for All Discovered Links in NE Group option, but only affects operationally down objects.
Remove	From a service tier contextual menu on the composite service topology map navigation tree, the Remove option deletes the service from the network in a composite service tier. In a composite service, deleting a service is not the same as removing a service from a composite service. Deleting a service removes the service from the 5620 SAM database. To avoid a service outage, be certain of the action that you are taking. See Procedure 74-10 for more information about removing a service from a composite service.
Remove Card	The Remove Card option deletes the card from the slot when the slot and everything contained in the slot is changed to administratively down.
Remove From Ring Group	The Remove From Ring Group option removes the specified device from the ring group. The devices are not deleted; they remain in the equipment view of the navigation tree.
Remove Ring Group	The Remove Ring Group option removes the specified ring group. The devices contained in the ring group are not deleted; they remain in the equipment view of the navigation tree.
Resync	The Resync menu option specifies that SNMP MIB and CLI information bases are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the device. Resynchronization does not impact the contents of the historical statistics database.

(5 of 6)

Option name	Description
Scripts	The Scripts option is available to users with the appropriate scope of command roles. This option allows you to associate scripts and templates to object types directly from the navigation tree or from map objects without having to navigate through the Scripts tool. The Scripts option displays a drop-down menu. You can choose from the Add Script and Manage Scripts option. The menu also lists Associated scripts and templates. The type of script or template is identified by the icon located to the left of the script or template name. • The Add Script option opens the Select Script(s) window. From this window you can associate existing scripts and templates to the selected object type. You can also edit and create scripts and templates from the Select Script(s) window. • The Manage Scripts option allows you to add and remove script and template associations with the selected object type. You can also access the Scripts option from the configuration form.(1) See "Creating and executing scripts" in the *5620 SAM Scripts and Templates Developer Guide* for more information.
Shut Down	The Shut Down option specifies that the selected object is changed to administratively down. The object's OLC state automatically changes to Maintenance if the "Enable Automatic OLC State change" parameter is enabled. See "5620 SAM component configuration" in the *5620 SAM System Administrator Guide* for more information.
Shut Down MC LAG	The Shut Down MC LAG option specifies that the MC LAG is changed to administratively down.
Shut Down Peer	The Shut Down Peer option specifies that the MC peer is changed to administratively down.
Soft Reset	The Soft Reset option resets the card. A soft reset is preferable to a reboot, as it results in minimal downtime. A soft reset causes the card to stop all processes it is running and restart.
Turn Up MC LAG	The Turn Up MC LAG option specifies that the MC LAG is changed to administratively up.
Turn Up Peer	The Turn Up Peer option specifies that the MC peer is changed to administratively up.
Turn Up	The Turn Up option specifies that the selected object is changed to administratively up. The object's OLC state automatically changes to In Service if the "Enable Automatic OLC State change" parameter is enabled. See "5620 SAM component configuration" in *5620 SAM System Administrator Guide* for more information.
View CCM	The View CCM option opens the properties form for the CCM which is associated with the selected CPM.
View CPM	The View CPM option opens the properties form for the CPM which is associated with the selected CCM.

(6 of 6)

Note

(1) The Scripts option may be located under the More Actions button if more than one option exists for the configuration form.

5.2 Basic navigation tree procedures

Use the following procedures to manage equipment using the navigation tree.

Procedure 5-1 To search for objects in the navigation tree

You can use the navigation tree to find specific objects such as NEs, shelves, cards, and ports for the physical and logical network views.

1 To search for an object using the expandable search panel:

- **i** Click on the Find button on the navigation tree or press CTRL+F. The search panel appears.
- **ii** Configure the parameters, as required. The parameters available for configuration depend on the selected view.
- **iii** Click on the Find button in the search panel or press Enter. The first matching object is selected and expanded in the navigation tree.
- **iv** To find additional matching objects, click on the Next button or press F3. The next matching object is selected and expanded in the navigation tree.
- **v** To return to the previous matching object in the navigation tree, click on the Previous button or press Shift+F3.
- **vi** If required, click on the Clear button to clear all parameters configured in step ii.
- **vii** To close the search panel, click on the Find button at the top of the navigation tree window or press CTRL+F .

2 To search for an object using the Find parameter at the top of the navigation tree window:



Note 1 — This step applies only to the equipment and routing views.

Note 2 — Up to 200 instances can be displayed at a time.

Note 3 — The Next and Previous buttons are enabled when more than one object meets the criteria.

- **i** Configure the Find parameter with the search criteria. For example, a number, an IP address, a name, a software version, or any attribute that has been defined in the label. See Procedure 4-3 for more information about customizing labels for a workspace.
- **ii** Press Enter. The first matching object is selected and expanded in the navigation tree.
- **iii** To find additional matching objects, click on the Next button or press F3. The next matching object is selected and expanded in the navigation tree.
- **iv** To return to the previous matching object in the navigation tree, click on the Previous button or press Shift+F3.

Procedure 5-2 To make a selected object the root of the navigation tree

Use the Make Root option of the contextual menu to make a selected object the root of the navigation tree. The Make Root option is only available in the Equipment view. See section 5.1 for information about the navigation tree objects that support the menu option.

The Make Root option of the contextual menu is not available for an object that is positioned one object level below the root of the tree. For example, in a navigation tree where the device is the root of the tree, the LAG object and the shelf object do not support the Make Root option.

Right-click on the navigation tree object that you want to make the root of the tree and choose Make Root from the contextual menu. The navigation tree is refreshed with the selected object as the root of the tree. The Make Root At Top Level button is enabled.

See Procedure 5-4 for information about restoring the default root of the navigation tree.

Procedure 5-3 To make a selected object the root of another navigation tree

Use the Make Root In New Tree option of the contextual menu to make a selected object the root of another navigation tree.



Note — Up to seven navigation tree windows can be open at the same time and each tree must have a different root when it is first created.

The Make Root In New Tree menu option is only available in the equipment view. The Make Root In New Tree option is not available in the contextual menu for the root object of a tree. See section 5.1 for information about the navigation tree objects that support the menu option.

Right-click on the navigation tree object that you want to make the root of another navigation tree and choose Make Root In New Tree from the contextual menu. Another navigation tree window appears with the selected object as the root of the tree.

Procedure 5-4 To restore the default navigation tree root

The default root of the navigation tree is the network object. When the root is not the network object, the Make Root At Top Level button is enabled.

Click on the Make Root At Top Level button in the navigation tree toolbar to restore the default root of the tree. See section 3.1 for more information about the Make Root At Top Level button.

6 — 5620 SAM topology map management

6.1 5620 SAM topology map management overview *6-2*

6.2 5620 SAM topology map types *6-14*

6.3 Working with topology maps *6-23*

6.4 Workflow to use 5620 SAM topology maps *6-26*

6.5 Basic 5620 SAM topology map procedures *6-27*

6.6 5620 SAM topology map configuration procedures *6-34*

6.7 5620 SAM topology map management procedures *6-44*

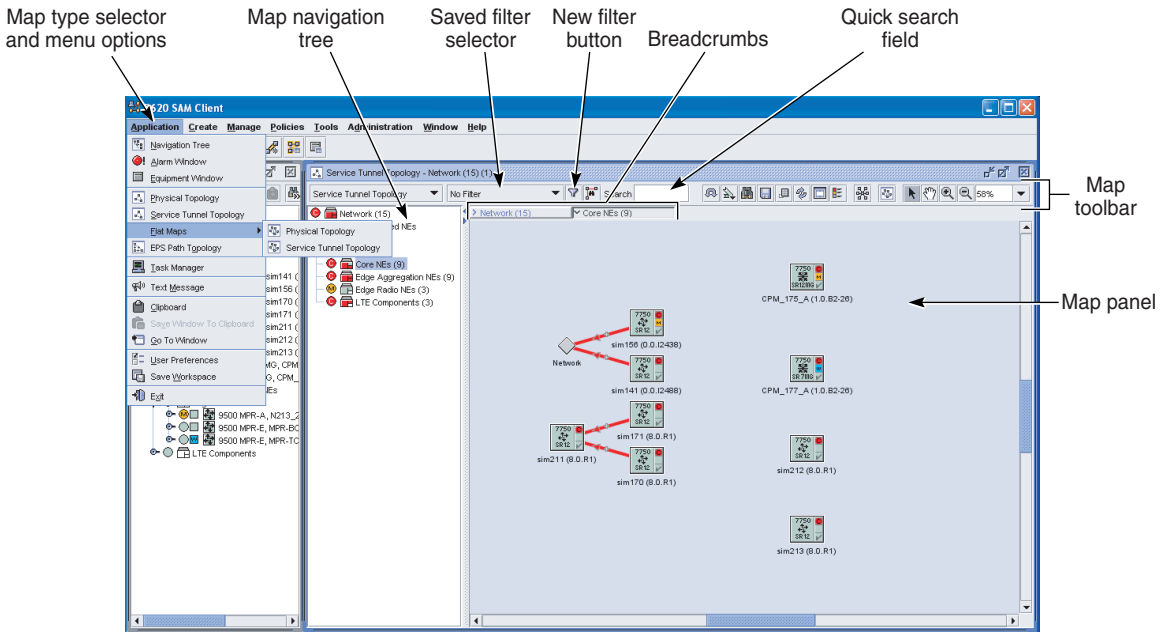
6.1 5620 SAM topology map management overview

The following 5620 SAM network topology maps are available:

- physical
- service tunnel
- service
- EPS path
- composite service
- LSP path
- LSP cross-connect

Each map displays network objects and information, and provides contextual menus to open forms that display additional information. In the context of a 5620 SAM map, a link object, such as a physical link or service tunnel, is called an edge. An object other than a link between objects, such as an NE or a topology group, is called a vertex. Figure 6-1 shows the main map elements.

Figure 6-1 Map elements



Map window

The map window includes the following:

- a title bar
- a map panel that displays the network objects
- a navigation tree that lists the topology groups
- a toolbar, which consists of a view selector, saved filter selector, quick-search field, and buttons that perform various functions

The title bar of the map window displays the following information:

- map type, for example, Physical Topology
- path from the network root to the currently displayed topology group; each step in the path is called a breadcrumb
- map number, for example, the first or the tenth map opened

Map panel

The map panel is associated logically with the map navigation tree. As the user navigates through the topology groups in the map navigation tree, the contents displayed on the map panel change. The topology group that is selected in the map navigation tree is the group that is displayed on the map panel.

When you double-click on a topology group object, the contents of the group on the map panel are displayed and the group is selected and opened in the map navigation tree. When you double-click on other map objects, such as routers or links, their property form opens. Right-click on any map object to display a contextual menu.

When map objects are linked between different topology groups, the line representing the connection terminates on a map object called a connector. The connector indicates that the endpoint of the link resides in another topology group. The label of the connector icon is the name of the topology group to which the link points. Connector objects do not have contextual menus.

When a physical link is created between a port or LAG managed by the 5620 SAM and an unmanaged object, the unmanaged object is called a remote endpoint. The remote endpoint label is configured by the user when the physical link is created.

You can configure a background image to display in the map panel for a topology group, for example, a map image of North America. You can position device icons and topology group icons in the map of the network to reflect their relative geographic locations.

Selecting map objects

Click on the Select Tool button to select an object on the map. To select multiple objects, press the Shift key and click on each object that you want to select, or draw a selection rectangle around all of the objects that you want to select on the topology map. You can also press CTRL-A to select all of the objects on a map.

You can select one or more objects and view them in a separate map by right-clicking on the selection and choosing Show Only Selected. The map is then filtered to display only the selected objects and the links between them. Links to other objects are excluded. To revert to the previous view, right-click in the map and choose Cancel Show Only.

When multiple objects are selected, you can press the F3 key to shift the map focus to the next object, and press CTRL-F3 to shift the map focus to the previous object.

You can also select all of the NEs that are attached to an NE by selecting one or more NE and right-clicking and choosing Select Attached.

To deselect a selected NE, press the CTRL key and click on the NE.

Moving map objects

The 5620 SAM allows you to move map objects in the following ways:

- in the map panel; for example, to add a router to a topology group by dragging and dropping the router object to the topology group object in the map panel
- from the map panel to the map navigation tree; for example, to add a router to a topology group by dragging and dropping the router object from the map panel to the topology group object on the map navigation tree
- after discovery by using either the or by moving the tiled icons to a new map panel location
- between two maps
- in the map navigation tree; for example, to make a topology group the immediate descendant of another topology group by dragging and dropping one topology group object to another topology group object in the map navigation tree

When a topology group is created, users with Topology Mgmt privileges can populate the group from the topology map by dragging and dropping map objects into the group in the map panel or in the map navigation tree, or from the map panel to the map navigation tree.



Note — You cannot move map objects to or from groups that are not within your span of control.

By default, users can move map objects and change the layout of the objects on the map, however the changes are not saved to the database when the map is closed. The ability to save changes to the layout of topology maps is controlled by scope of command roles and access permissions. Permissions are set by using 5620 SAM security configuration forms. See "5620 SAM user security tasks" in the *5620 SAM System Administrator Guide* for more information about setting access privileges.

The Reload button icon indicates when you move a map object and change the layout of the objects. The Reload button icon changes to indicate whether moving a map object and changing the layout of the objects is saved to the database. See "Map toolbar" in this section for more information about the Reload button.



Note — When you move a map object in the map panel, the X,Y coordinates for the map object change. If you have update and execute scope of command access permission, this change affects all users that display the map view and the topology group.

Connectors can only be moved in the map panel. Connectors cannot be moved to another topology group.

Finding map objects quickly

The Search field beside the toolbar buttons allows you to quickly locate a map object. When you enter a text string in the Search field and press ↵, the 5620 SAM searches each object name in the map for the string. If a match is found, the map focus shifts to the object. If multiple matches are found, you can press the F3 key to shift the map focus to the next object, and press CTRL-F3 to shift the map focus to the previous object.

Links and link groups

The topology maps display single links and multiple links that connect two map objects. Links are used to represent the physical connectivity between two NEs or logical connectivity, such as service tunnels. The map uses an arrow to display the direction of a unidirectional link. Multiple links between 2 objects are grouped, by default, as one link with no defined direction. Bidirectional links are displayed with no defined direction. A link group is displayed with a plus sign located on the link object. You can right-click on the plus sign and choose Expand Group to view all of the associated links. The expand threshold of links on the topology maps displays up to 10 links.

When you double-click on a single link, the properties form for the link opens. When you double-click on the link group object for multiple links, a list form opens displaying all of the links that belong to the link group. For the physical, service tunnel, and LSP maps, a list form opens regardless of whether there is one link or multiple links in the link group.

A bidirectional link group is displayed with a plus sign icon located in the middle of the link object. A unidirectional link or link group is displayed using an arrow icon on the object pointing in the direction of the path.

The color of a single link object is determined by the status of each link endpoint. The color of a link group object is determined by the most serious alarm that is raised for a link in the link group.

Breadcrumbs

Breadcrumbs are buttons that are displayed along the top of the map panel. Breadcrumbs indicate, from left to right, the hierarchy of the topology groups to the group currently displayed in the map panel. The default top of the hierarchy, the breadcrumb at far left, is the entire network. Click on a breadcrumb to open the map for the corresponding group.

Map navigation tree

The following network topology maps display a map navigation tree:

- physical map
- service tunnel map

You can use the map navigation tree:

- for non-linear navigation to any topology group on the map
- to display the topology group hierarchy starting from the entire network

The map navigation tree displays:

- topology groups, including group names
- status of the topology groups

When you click on a map object in the map navigation tree, the contents of the object are displayed in the map panel, and the map object is selected. See section 5.1 for more information about the navigation tree.

Contextual menus for objects in the map navigation tree

To open a contextual menu for an object, right-click on a map object in the map navigation tree. See Table 5-2 for more information about contextual menu options.

Map toolbar

The map toolbar allows you to manage a 5620 SAM map view. The toolbar is above the map panel in the map window. Figure 6-2 shows the map toolbar elements.

Figure 6-2 Map toolbar elements

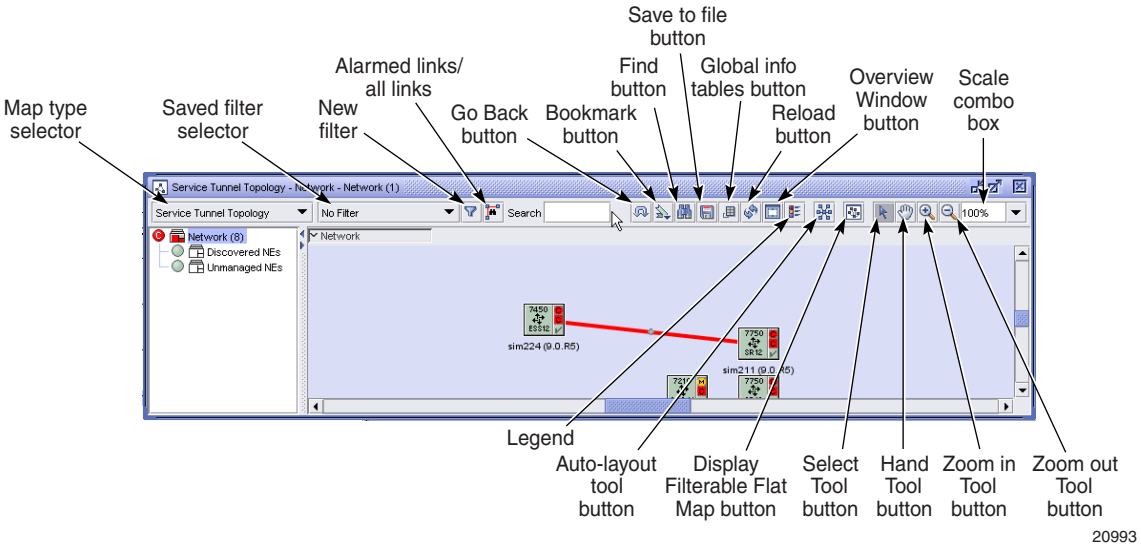


Table 6-1 describes the map toolbar elements.

Caution 1 — Applying an information table configuration to many objects on the map may take a long time.

Caution 2 — When you reload a map from the database, the database is unavailable during the loading period.

Caution 3 — The current composite service map is redrawn when you click on the Rearrange by Service Tiers button, and the prior layout of the composite service map cannot be recalled.

Caution 4 — After you click on the Auto-Layout Tool button and confirm the action, any existing map layout is overwritten and cannot be recovered. If you are satisfied with the layout of the icons on the map, do not use the Auto-Layout Tool button.

Table 6-1 Map toolbar elements descriptions

Toolbar element name	Description
Map type selector	The map type selector is a drop-down menu that lists the map view options that you can choose to specify the view. The map type selector offers the following views: • Physical Topology • Service Tunnel Topology
New Filter button 	A filter allows you to apply one or more object filters to a map view, to narrow the range of objects that are displayed. Filters can be saved for future searches on similar objects. When a filter is applied, the name of the filter is displayed on the saved filter selector. Only the objects that the filter returns are displayed, with the following exceptions: • If one link endpoint is displayed, the other endpoint is also displayed, even when the filter excludes the endpoint. • If a filter does not include a link filter, only the links between the returned NEs are displayed. Filters can be saved as private or public. You can apply a span of control to public filters to filter out objects that are not in the current user span of control. Public filters can only be changed by the user who created them. Private filters appear only for the user who creates them. Click on the Filter button to create and save filters that specify the objects displayed in a map. You can create a filter based on a combination of search criteria. Figure 6-4 shows the navigation buttons that you can use to create, apply, and save a map filter. See Procedure 6-20 for more information about creating a topology map filter. See chapter 3 for more information about configuring filters.
Alarmed links/All links shown button 	Click on the Alarmed links/All links shown button to specify any of the following on the topology map: • all links • only link groups with associated alarms • only specific links with associated alarms • link groups and the specific links within the link groups with associated alarms The Alarmed links/All links shown button options are: • All links shown (default)—the icon is displayed in white and all links are displayed on the map. • Show Only Alarmed—the icon is displayed in yellow and only link groups with associated alarms are displayed on the map. • Enable Alarm Link Pullout—the icon is displayed in yellow and links with associated alarms are displayed on the map. The link groups containing the pulled out alarm links with unknown physical characteristics are displayed in grey.
Go Back button 	Click on the Go Back button to navigate between previously viewed topology groups. For example, if you are viewing Router Group 1 then view Router Group 2, click on the Go Back button to return to Router Group 1. The Go Back button only functions in one map type; both previously viewed topology groups must be the same map type.
Bookmark button 	Bookmarks are used to create shortcuts to frequently visited locations on a map. Click on the Bookmark button and choose to add a bookmark or manage existing bookmarks.
Find button 	Click on the Find button to search for network objects on a map. You can choose to search for specific vertices or edges. A list form opens that allows you to configure specific criteria to filter the results of your search. See chapter 3 for information about performing searches. When the network object is found, the map navigation tree displays the topology group that contains the object. If necessary, the 5620 SAM scrolls to the part of the map where the object is located.

(1 of 3)

Toolbar element name	Description
Save To File button 	Click on the Save To File button to save the map view or the full map. You can choose the location to save the map image and the file type. See Procedure 6-8 for more information about using the Save To File button.
Global Info Tables button 	Click on the Global Info Tables button to create information table configurations, apply information table configurations globally, or turn the global information table option off. See Procedures 6-14 and 6-15 for more information about using the Global Info Tables button. See Caution 1 above.
Reload Button indicating no database changes  Reload Button indicating database changes 	Click on the Reload button to load the topology map from the 5620 SAM database. The topology map is updated to display the latest configurations. The Reload button icon changes to indicate whether moving a map object and changing the layout of the object is saved to the database. See Caution 2 above.
Overview Window button 	Click on the Overview Window button to open the Overview window. Use the Overview window to pan the entire map, or a specific group or service, and the area that you want to view. Figure 6-3 shows the Overview window.
Legend button 	Click on the Legend button to open a contextual menu that displays a list of map legend types if multiple legends are available, or opens the Legend form. Choose a legend type from the contextual menu to open the Legend form with the appropriate legend tab displayed. Depending on the map type, the following legend types are available: • icons—displays the icons used to identify objects; always appears • colors—displays the color scheme used to identify map objects • highlight sessions—displays the highlight sessions for the current map, and allows you to clear one or more sessions • other legend types that apply to a type of map
Rearrange by Service Tiers button 	The Rearrange by Service Tiers button is available only for composite service topology maps. Figure 6-13 shows the composite service map. Click on the Rearrange by Service Tiers button to organize the composite service tier icons in the map panel by service tier. The service tier icons are displayed in the following order from the top of the panel: • tier 1 icons (typically IES and VPRN services) • tier 2 icons (typically VPLS and MVPLS) • tier 3 icons (typically satellite HVPLS and VLL services) • tier 4 icons (typically VLAN services) . . . • tier n icons (user-assigned) See Caution 3 above.

(2 of 3)

Toolbar element name	Description
Auto-Layout button[1] 	Click on the Auto-layout button to lay out the map icons. The layout options are: • Circular — emphasizes ring and star topologies in networks. Objects are grouped according to the network structure and arranged in circles or radial tree structures. • Smart Organic—emphasizes inherent data groupings and symmetries. This information helps with understanding the interconnections of complex structures. • Endpoint Layout (VPLS, VLL, mirror, and composite service sites only) - all endpoints are snapped close to the associated parent site. The Auto-Layout tool is useful when: • many newly discovered NEs are tiled together on the map and difficult to view • a large number of network device icons are spread out across the map and cannot be easily viewed without zooming out After you click on the Auto-Layout button, icons with links between them are placed closer together in the center of the map. Icons without links are placed on the periphery of the linked icons. See Caution 4 above.
Display Filterable Flat Map button 	Click on the Display Filterable Flat Map button to quickly display a flat map of the current topology map view. You can also view a flat map on the 5620 SAM by choosing Application→Flat Maps from the 5620 SAM main menu.
Select Tool button 	Click on the Select Tool button to select and move an object on the map or to view object information. You can select and move multiple objects by pressing the Shift key and clicking on each object you want to select, or by drawing a selection rectangle around all the objects you want to select on the topology map.
Hand Tool button[2] 	Click on the Hand Tool button to switch to a pan mode. Click on the background to move the contents of the map in any direction. When you are in the pan mode and you scroll over an object, you can select and move an object on the map or view object information. You can select and move multiple objects by pressing the Shift key and clicking on the object you need to select.
Zooming in  and zooming out  using a mouse or toolbar buttons[3]	The ability to zoom in and out on a map allows you to view hundreds of map objects at once to see the scope of the network, or view the information for one NE. Click on the Zoom in Tool and Zoom out Tool buttons and click on the map to resize the objects in a map or use the mouse wheel to zoom in and zoom out of topology maps. Click on the map and roll the mouse wheel forward to zoom in or roll the mouse wheel backward to zoom out. Each roll of the mouse wheel brings the map objects closer or further. When a map is at a low zoom level, the icons are displayed at a reduced size, link lines are thinner and labels are hidden. Labels are displayed when you click on the reduced icon. When a map is viewed at a high zoom level, the icons are displayed at normal size, link lines are thicker and labels are displayed.
Scale combo box	Use the scale combo box to increase or decrease the map zoom. You can choose a zoom percentage value from 25% to 300%, or fit all objects in the window from the drop-down menu. The scale combo box displays the current scale of the map.

(3 of 3)

Notes

(1) You can also apply the auto-layout option to a contiguous group by right-clicking on one of the selected objects. See Procedure 6-22 for information about using the auto-layout function.

(2) To temporarily activate the panning function, press and hold the space bar, and then click in the map panel.

(3) Object icons are displayed at a reduced size in a flat map.

Figure 6-3 shows the Overview window.

Figure 6-3 Overview window

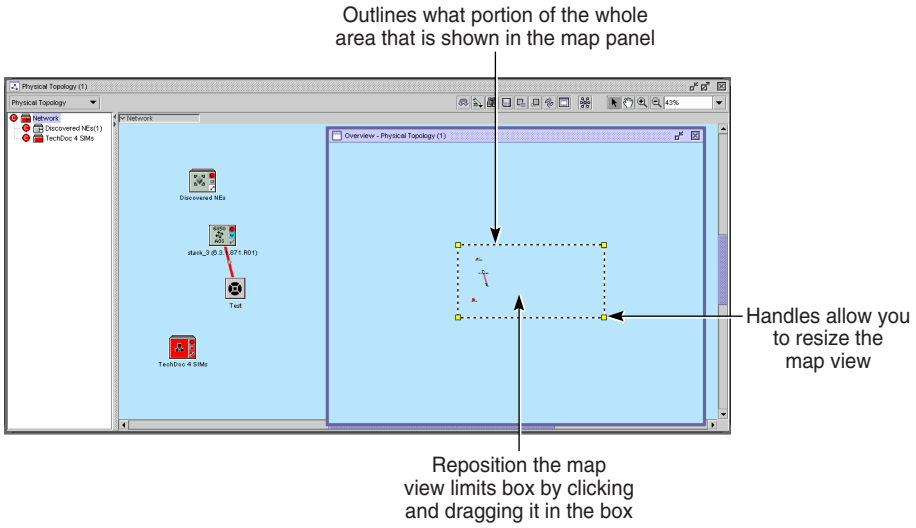
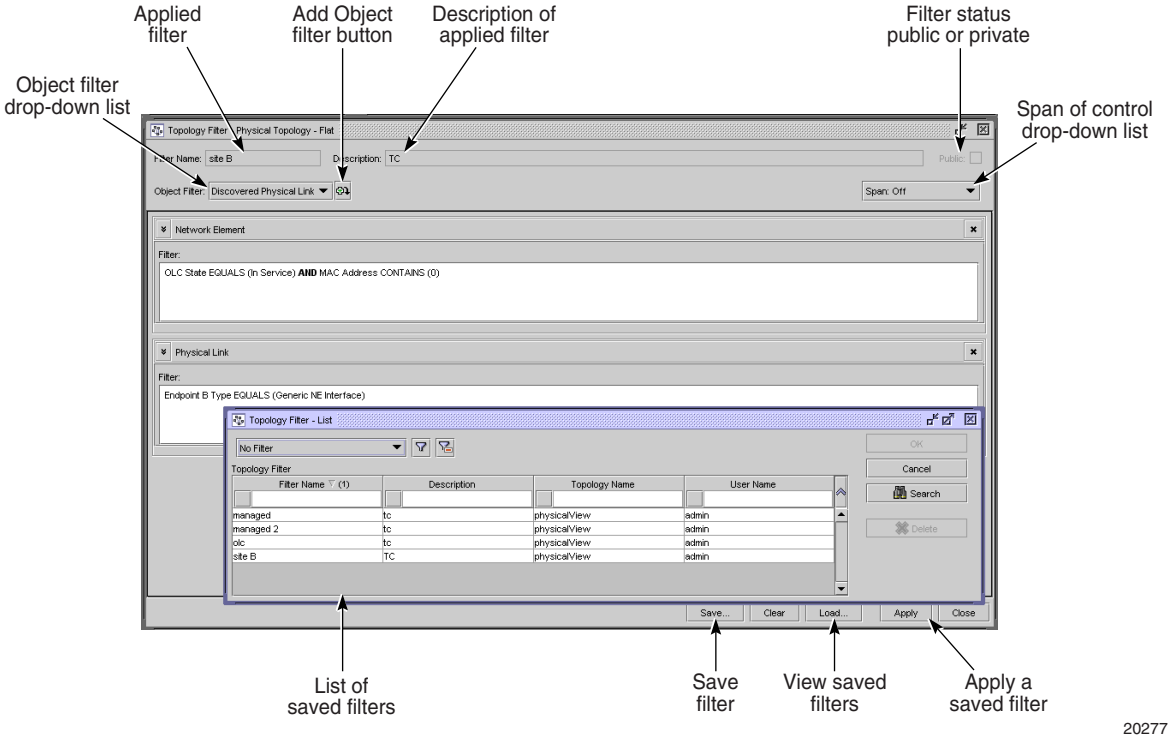


Figure 6-4 shows the navigation buttons that you can use to create, apply, and save a map filter.

Figure 6-4 Filtered map form



Zooming in and out

The ability to zoom in and out on a map allows you to view hundreds of map objects at once to see the scope of the network, or view the information for one NE. See Procedure 6-11 for information about zooming functions.

When a map is viewed at a low zoom level, the icons are displayed at a reduced size, link lines are thinner and labels are hidden. Labels are displayed when you click on the reduced icon. When a map is viewed a a high zoom level, icons are displayed at normal size, link lines are thicker and labels are displayed.

Bookmarks

You can bookmark frequently visited areas of the map for easier navigation when you return to those locations. Bookmarks are associated with a map view. To use the bookmark, you must be in the same view where you created the bookmark or a view that shares the same group, for example, a topology group that belongs to both the physical topology map and the service tunnel map. Otherwise, the bookmark menu option is disabled.

You can access the bookmark drop-down menu using the Bookmark button on the map toolbar. Figure 6-2 shows the Bookmark button. The bookmark menu is divided into two sections and separated by a horizontal line. The top section of the drop-down menu contains the bookmark management functions, and the bottom section contains the user-created dynamic list of bookmarks.

The list of bookmarks is updated when you add, remove, group, or rearrange the bookmarks. The menu items can be bookmarks or folders, which can expand to display more bookmarks or folders.



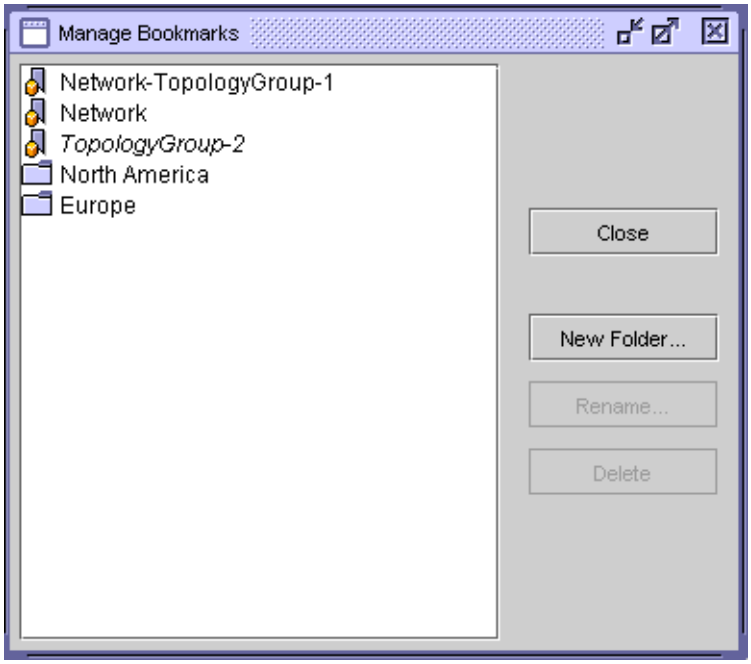
Note — A large number of bookmarks is difficult to manage. Bookmarks should be organized in folders for better usability and easier management. Alcatel-Lucent recommends that you create a maximum of 1000 bookmarks.

When a bookmark is selected, the map panel displays the bookmarked topology group. The map navigation tree expands to display the topology group.

When a valid bookmarked topology group is moved to another group, the bookmark for the group is updated to correspond to the new location of the group. If the bookmark location is not valid, for example, a topology group was deleted since the bookmark was created, an invalid bookmark message is displayed. The map panel remains unchanged.

Click on the Add Bookmark menu option to add the topology group currently viewed in the map panel as a bookmark. Click on the Manage Bookmarks menu option to open the Manage Bookmarks form. Figure 6-5 shows the Manage Bookmarks form.

Figure 6-5 Manage Bookmarks form



The Manage Bookmarks form has a list panel on the left in which the bookmarks and folders are listed in a tree structure. You can drag and drop bookmarks and folders in and out of other folders in the list panel. Select a bookmark or folder for editing. Click on an empty area to deselect the tree object. Double-click on a top-level folder to open the folder and display its contents. A turner to the left of the descendant folder object in the list panel indicates that the folder contains descendant objects, such as bookmarks or other folders.

The names of invalid bookmarks, and bookmarks and folders that are not from the current view, are displayed in italics.

The following buttons with which you can perform different actions are displayed to the right of the list panel:

- Close—used to close the Manage Bookmarks form. All changes in the form are saved when you click on the Close button.
- New Folder—used to create a folder in the list panel. The Folder Properties dialog box appears.
  - If a folder is selected in the list panel, the new folder that is an immediate descendant object of the selected folder.
  - If no folder is selected in the list panel, the new folder is created as a top-level folder.
- Rename—used to rename a folder or bookmark. The Rename dialog box appears. The Name field contains the name of the selected folder or bookmark. This button is enabled only when a folder or bookmark is selected in the list panel.
- Delete—used to delete a selected folder or bookmark from the list panel. This button is enabled only when a folder or bookmark is selected.

Information tables

You can configure information tables that are displayed beside map objects. An information table contains specific values, such as an NE chassis type, software descriptor, and system address. Information tables are displayed beside each map object to which the configuration applies. You can drag and drop information tables on topology maps, but the new table location is not saved with the map.



Note — You cannot apply an information table configuration to link groups or topology groups.

Multiple information tables can be applied to map objects, but only one table is displayed at a time. Tab indicators appear on the information table to indicate that multiple information tables apply to the map object. To cycle through the applied information tables, click on the information table and press the Tab key.

You can specify that information tables are displayed only during a mouse-over operation, which is when the mouse pointer passes over an object. You can also specify whether an information table contains a header. Header display is enabled by default and cannot be disabled for mouse-over tables. See Procedure 6-14 for more information. Mouse-over supports cycling between tables by pressing the Tab key.

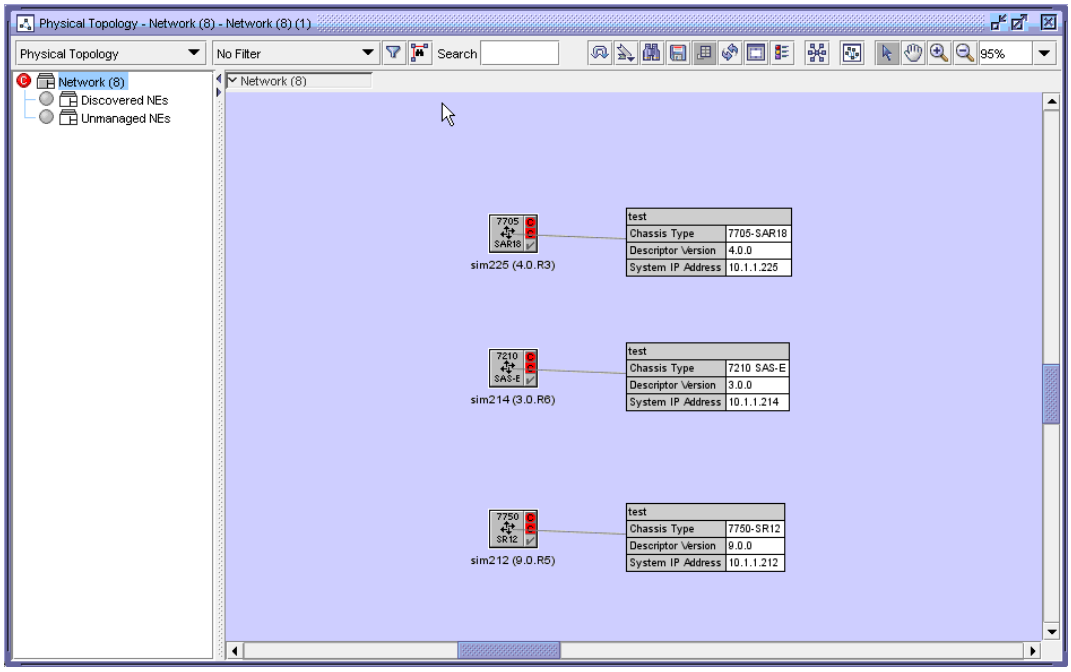
The following types of information tables can be applied to map objects:

- global—available for all map types
- selected—available for all map types
- highlight—available for maps that support the highlight function
- others that apply to a specific map type

Global Info Tables

When one or more information table configurations are available for a map type, you can apply an information table configuration to all map objects using the Global Info Tables button. You can also use this button to turn the global information table configuration off. See Procedure 6-15 for more information about how to use the Global Info Tables feature. Figure 6-6 shows a map view with an information table configuration applied to all map objects.

Figure 6-6 Applied global information table configuration



Selected Info Tables

You can apply an information table configuration to one map object or a selected group of map objects by right-clicking on the object or selected group. You can also use this contextual menu to turn the selected information table configuration off. See Procedure 6-16 for information about how to use the Selected Info Tables feature.

Map Highlight Info Tables

On a map that supports the highlight function, you can apply an information table configuration to a map highlight by right-clicking on an existing highlight session from the Highlight Sessions tab of the Legend-*topology* form. You can also use this contextual menu to turn the highlight information table configuration off. See Procedure 6-17 for more information about how to use the Map Highlight Info Tables feature.

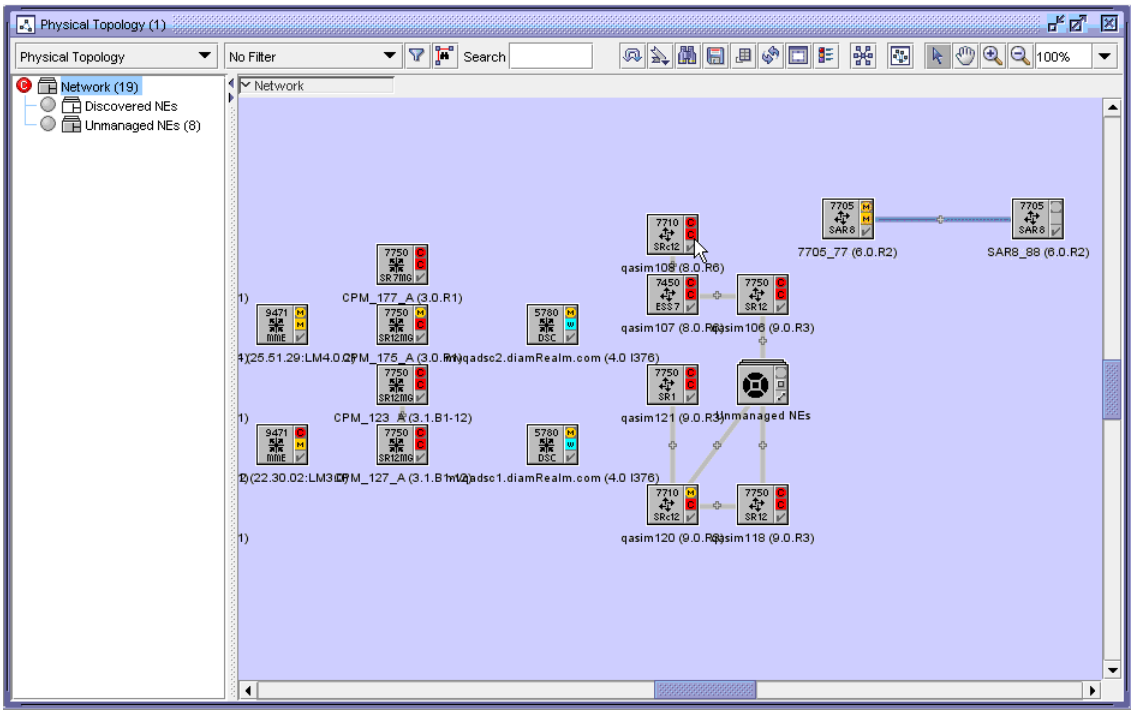
6.2 5620 SAM topology map types

This section details the types of maps available to the 5620 SAM.

Physical topology map

The physical topology map is available by choosing Application→Physical Topology from the 5620 SAM main menu. The physical topology map is used to view and manage Layer 1 objects, including the logical grouping of devices. Figure 6-7 shows the physical topology map.

Figure 6-7 Physical topology map



The physical topology map is open in the working panel by default when the 5620 SAM client GUI starts.

The following apply to link objects in the physical topology map:

- The following colors indicate link status:
  - Red—the link has failed
  - Light gray—the link is in service
  - Green—the link is new
  - Blue—the link is in standby or backup mode
  - Dark gray—the link is unknown
  - Purple—the link is being diagnosed
  - Magenta—the link carries hidden links
  - Yellow—the LAG link is degraded (one or more links in the LAG have failed)
- For aggregated 1+1 HSB microwave radio links on a 7705 SAR, the following colors indicate link status:
  - Red—the MW radio link is down
  - Blue—the MW radio link is up
  - Yellow—the MW radio link has a problem
- For expanded, unidirectional 1+1 HSB microwave radio links on a 7705 SAR, the following colors indicate link status:
  - Red—the unidirectional radio link has a problem and the MW radio link is down
  - Green—the MW radio link is in service
  - Blue—the MW radio link is in standby mode
  - Yellow—the unidirectional radio link has a problem but the MW radio link is up

- If endpoint B of a physical link is on an unmanaged device, the status of the physical link is the same as the status of endpoint A, which is on a 5620 SAM-managed device.
- A LAG link is represented as a single physical link. However, if you right-click on a LAG link, the form that opens provides information and configuration options for the entire LAG link. For example, the Endpoint Info tab on the Discovered Physical Link form shows the link endpoints as LAG endpoints rather than physical ports, and allows the operator to open the LAG properties form.

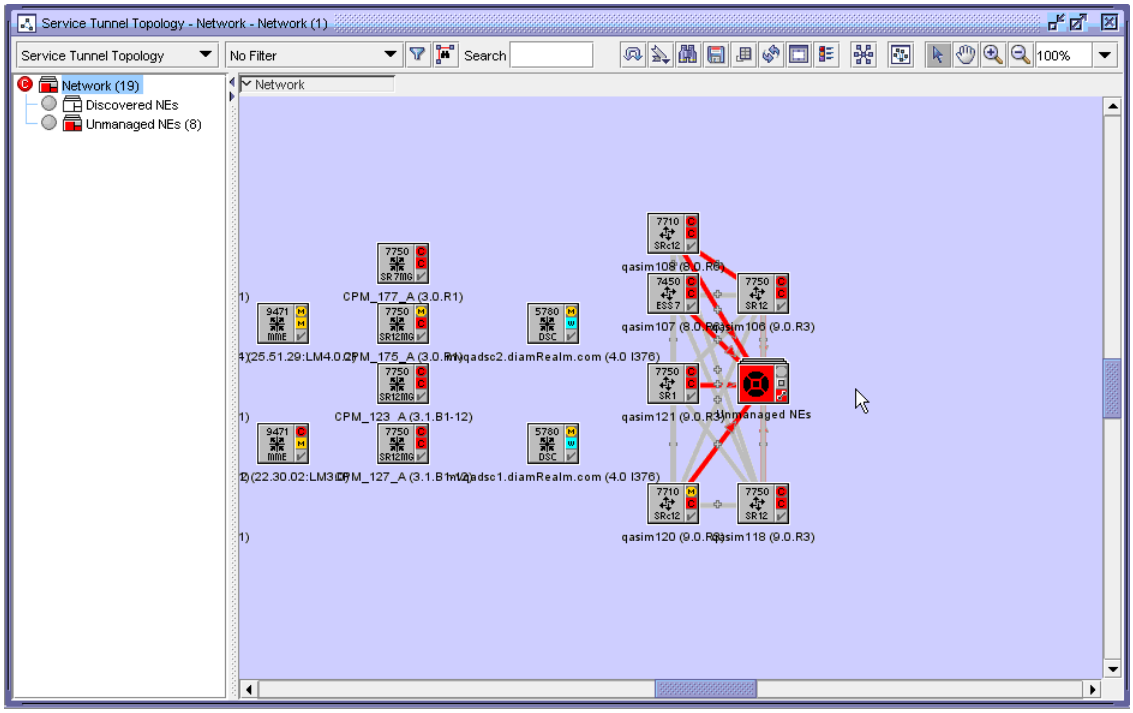
Menu options for physical topology map background

To open a contextual menu for the map background, right-click on the map background. See Table 5-2 for contextual menu option information.

Service tunnel topology map

A service tunnel topology map is available on the 5620 SAM by choosing Application→Service Tunnel Topology from the 5620 SAM main menu. The Service Tunnel Topology map is displayed, as shown in Figure 6-8.

Figure 6-8 Service tunnel topology map



Icons in the service path topology map represent devices. The color of the device icon represents the status of the device. Red means that the device is down. Green means that the device is up. Yellow means that the device is being synchronized. Purple means that the device is in a suspended management state. See chapter 10 for information about device discovery and management states.

Link groups between devices represent service tunnels. When a link group is red, at least one tunnel in the link group is down. For link groups between managed devices, right click on the link group icon to list and edit tunnels in the link group. For link groups between managed and unmanaged devices, right-click on the link group icon to open contextual menus and submenus which allow you to open additional information forms for the service tunnel, including the properties form.

EPS path topology maps

An EPS path topology map is available on the 5620 SAM by choosing Application→EPS Path Topology from the 5620 SAM main menu. The EPS path topology map displays a static representation of mobile network objects and EPS paths. Each network object icon represents an aggregate of all network objects of that type. For SGWs and PGWs, the icon represents an aggregate of all instances of that gateway type and all network objects that contain instances of that type. Each EPS path link represents an aggregate of all EPS paths of a specific type.

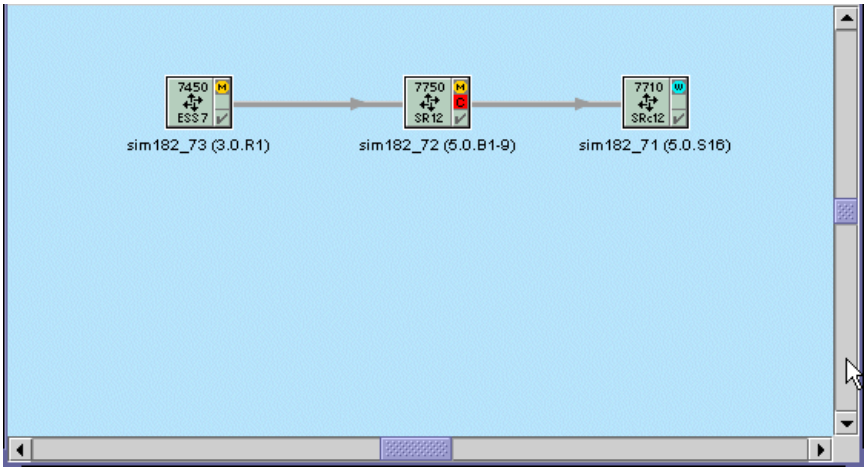
See the *5620 SAM LTE EPC User Guide* and the *5620 SAM LTE RAN User Guide* for information about EPS paths in LTE networks.

LSP path topology map

An LSP path topology map is available from the MPLS Path form and the LSP Path form. See Procedure 6-3 to view the map from the MPLS Path form. See Procedure 6-4 to view the map from the LSP Path form.

The LSP path topology map is used to view a specific provisioned, actual, or CSPF LSP path in the context of its source, and transient and destination hops. Figure 6-9 shows an LSP path topology map.

Figure 6-9 LSP path topology map



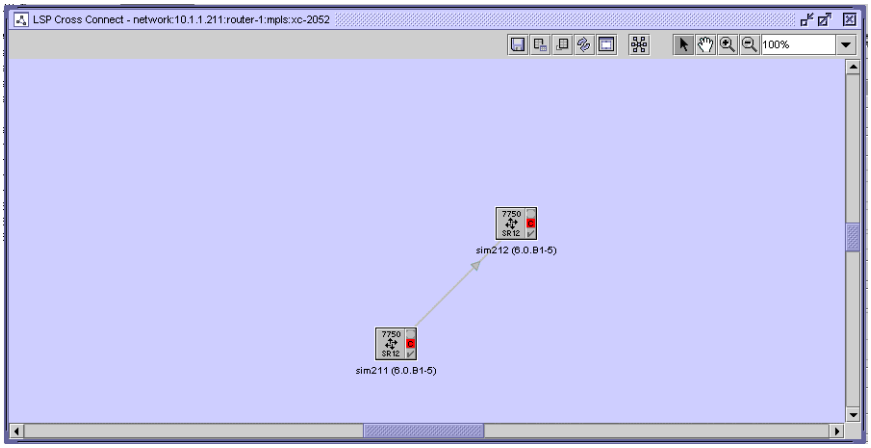
When you view the LSP path topology map, hops are linked by straight lines, where each line represents a sub-path between two hops of the LSP path. The direction of each path is indicated by an arrow. Green lines indicate provisioned paths, and gray lines indicate actual paths.

LSP cross-connect topology map

An LSP cross-connect topology map is available from the LSP Path form. To view the map from the LSP Path form, see Procedure 6-6.

The LSP cross-connect topology map is used to view a specific LSP cross-connect in the context of its source, and transient and destination hops. Figure 6-10 shows the LSP cross-connect topology map.

Figure 6-10 LSP cross-connect map



Flat maps

Flat maps provide a complete network view without topology groups. A flat topology map can display up to 1000 objects. You can narrow the range of objects that are displayed by creating and saving filters and filter definition trees.

A flat map is available on the 5620 SAM by choosing Application→Flat Maps from the 5620 SAM main menu. The following flat map types are available:

- Physical Topology
- Service Tunnel Topology

A flat map is used to view a large number of network objects and link groups. You can double-click on a NE in the flat map to display the object properties. For example, when you double-click on an NE, a property form opens, from which you can view or configure the NE parameters.

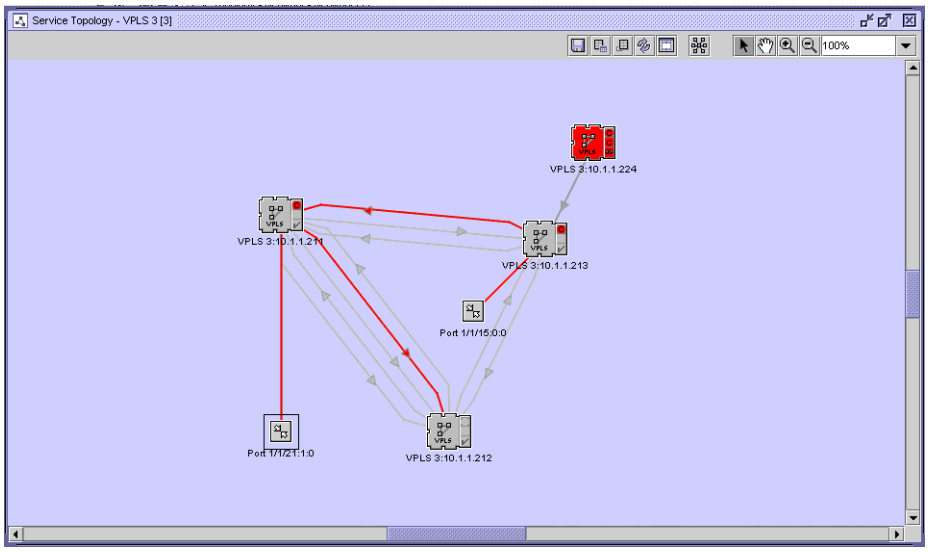
Object icons in a flat map are displayed at a reduced size, link lines are thinner, and object information is not displayed. Flat maps support the following, as do other 5620 SAM topology maps:

- mouse-based navigation
- zooming
- NE and link status colors
- searching
- filtering

Service topology maps

You can open a topology map for a selected service from the Manage Services form by clicking on the Topology View button. Figure 6-11 shows a service topology map. Large NE icons represent managed devices. Small NE icons represent unmanaged devices. The label of an NE icon indicates the service name and the NE IP address.

Figure 6-11 Service topology map



The symbol and color in the top-right corner of the managed device icon represents the aggregated alarm status, which is the most severe alarm on any service that includes the device. The symbol immediately below the aggregated alarm status and the color of the icon indicate the alarm status for the currently displayed service site. A red icon indicates that the service site is down. A green icon indicates that the service site is up.

A port icon represents a managed access interface. A port label includes the port number and the inner and outer port encapsulation values. A service site can support up to 20 SAPs. When the number of SAPs on a service site exceeds 20, the SAPs on the site are grouped into a SAP group, represented by a SAP group icon. When the number of SAPs drops below 20, the SAP group icon is replaced with the icons for the individual SAPs. To view the list of SAPs in a SAP group, right-click on the SAP group icon and choose List L2 Access Interface or List L3 Access Interface, depending on the service type. The corresponding Site form for the service opens with the L2 Access Interface or L3 Access Interface tab displayed.

SAP aggregation group icons represent SAP aggregation groups configured for a VLL Apipe on the 7705 SAR. The SAP aggregation group is linked to the service site and each of the individual SAPs. To hide the associated SAPs for a SAP aggregation group, right-click on the SAP aggregation group icon and choose Hide SAPs. Choose Show SAPs to show them again.

A line between two map objects represents a link or group of links. Links between device icons represent service circuits. Links between device icons and port icons represent the binding of an access port or interface to a service. The symbol and color in the bottom right corner of the managed device icon represents the connectivity alarm status. During a resynchronization of the managed device, the icon represents the resynchronization status, and is yellow. The status is inherited from the link endpoints. A plus sign icon located in the centre of the link indicates a bidirectional group link. An arrow icon located on the link indicates a unidirectional link and identifies the direction of the path.

Right-clicking on a managed site, port, or link opens a contextual menu that allows you to perform functions that include the following:

- choose layout options
- open an object properties form
- turn up or shut down an object
- create a service object
- create a service object from a template, if a template is bound to the service
- delete an object
- open a CLI session
- manage scripts
- plot statistics
- display or highlight service topology features

You can view multiple services on a map at the same time if the services are selected from the Manage Services form during map creation.

Service segmentation

A service segmentation view is also available to aid in conceptualizing complex services. Segments are logical grouping of interconnected sites, services, and bindings. The segmentation view is available for VPLS and VLL services.

A service segment is considered to be a portion of a single service that extends to multiple sites connected within that segment. It is based on the service type through one of the possible connection topologies (for example, mesh, PBB tunnels, a switching VLL, rings, and so on), without having to pass through any connectors such as spokes, CCAGs, or SCPs (SAP-to-SAP).

General examples of segments in Layer 2 service topologies include:

- A simple pair or single spoke/mesh SDP binding comprises one segment
- A mesh of a multi-NE VPLS service comprises one segment
- A multi-NE mesh with a spoke SDP to a single NE comprises two segments
- Each mesh of VSIs forms a segment (applicable to H-VPLS)

Just a few examples of the many possible service-specific segmentation configurations include scenarios such as the following:

- H-VPLS (Inter-Metro with redundant spoke SDPs):
  - One application of H-VPLS is the connection of two or more geographically-dispersed VPLS domains belonging to the same customer. Two spoke SDP connections are used to connect each VPLS between the two metros, either in a redundant PW spokes topology or under STP protocol. The redundant spokes comprise one segment, while each VPLS will also comprise one or more segments, depending on their specific configurations.
- VLL Switching:
  - For a VLL service at a switching router, a terminating PE device has at least one VLL SAP, while a switching PE device has a VLL instance which cross-connects two spoke bindings. All VLL instances of such a service must have the same service ID, and if the VLL has one or more switching sites, it must have at least two terminating sites. In this scenario, the primary and redundant spoke SDPs on the same network endpoint are considered to be in the same segment.
- PBB:
  - In a PBB configuration, the B-VPLS is considered a service tunnel, from the I-VPLS or I-Epipe perspective. Therefore, the sites connected via a B-VPLS (that is, having the same ISID) are considered to be in one segment.
  - I-Sites bound to the same PBB tunnel (B-VPLS) and having the same ISID exist in the same segment.
  - Epipe sites bound to same PBB tunnel (B-VPLS) exist in the same segment

Whenever you modify a service, the following actions can trigger segment creation, modification, or deletion in a segmented service view:

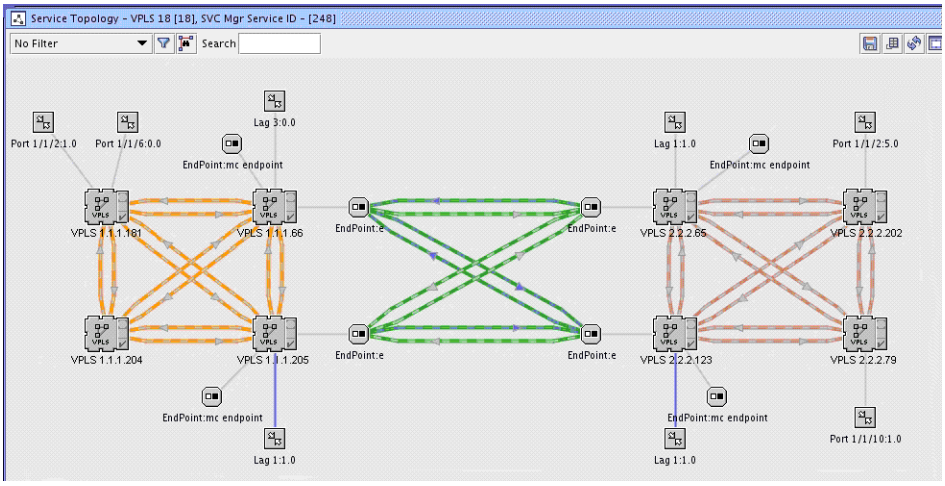
- Adding or removing service sites
- Creating or deleting spoke and/or mesh bindings (either through the 5620 SAM GUI or CLI)
- Creation or deletion of VLAN Uplinks by 5620 SAM

You can access the segmented view of a service by right-clicking on an empty portion of the background in the service's topology view. A contextual menu allows you to activate or de-activate the segmented view for the service.

In a segmented view, the outlined links of all spoke bindings, mesh bindings, or VLAN Uplinks are colored in the same distinct way for the segment they belong to. However, there are currently only 19 different colors available for use in showing service segments. If all the colors for a specific service are used, a warning message is logged to indicate this.

Figure 6-12 shows an example of how the 5620 SAM displays the segmented view of an H-VPLS Metro-to-Metro service.

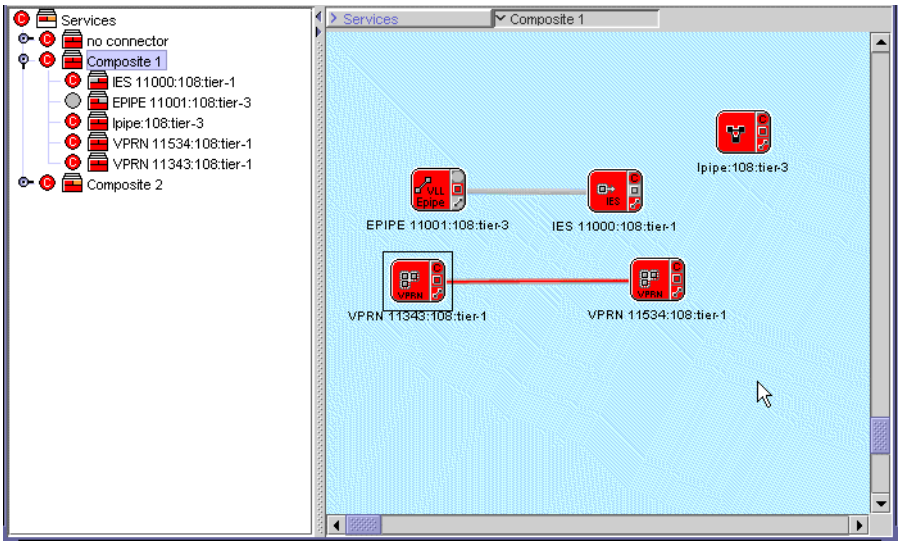
Figure 6-12 Service segmentation example



Composite service topology maps

You can use the 5620 SAM to view composite service topology and flat topology maps. Figure 6-13 shows a sample composite service topology map. When you open a flat topology view map, the navigation tree is not part of the map.

Figure 6-13 Composite service topology map



In a composite service topology map, you can use the navigation tree at the left side to display the composite service and service tier hierarchy starting from the services object. The map navigation tree displays the following:

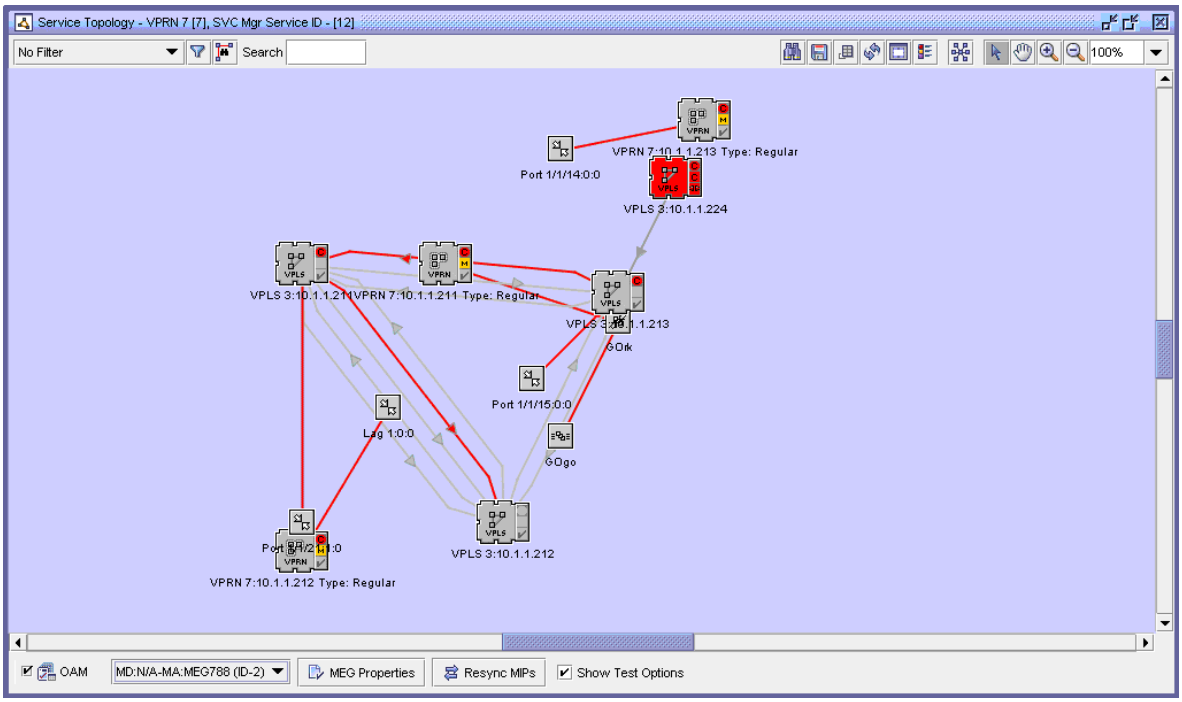
- composite services and service tiers, including service name and tier number
- status of the composite services and their tiers

The map toolbar for the composite service topology map includes the Rearrange by Service Tiers button. See Table 6-1 in this section for more information.

Double-click on a composite service object in the map panel to display the service objects that belong to the composite service. Double-click on the service objects to display the service sites and access interfaces. The links or groups of links between the service sites and access interfaces are also displayed.

In the composite service topology map, all service objects in the composite service are displayed simultaneously. The service sites, access interfaces, and the links or groups of links between them are also displayed. The navigation tree is thus not required in this view. Figure 6-14 shows a sample composite service flat topology map.

Figure 6-14 Composite service flat topology map



You can right-click on an object icon or link group icon to turn up, shut down, or display the properties form for the item.

You can also perform Ethernet CFM diagnostics directly from the composite service flat map.

6.3 Working with topology maps

This section details different methods of managing 5620 SAM capabilities from the topology view.

Modifying a service from the topology view

The topology view for a service provides a graphical representation of the various components and their interconnections. You can also use this view to add, modify, or just navigate to service components. This provides an alternative approach to performing these functions from the navigation tree view in the service configuration forms.

Working from the topology view can expedite the creation of the components, since many of the fields you would ordinarily have to set in the configuration forms will be automatically populated using this approach. The configuration forms can also be accessed directly at any time from this view by right-clicking a component. This allows quick access to conduct more detailed component configuration.

Services that can be modified from their topology views include VPLS, VPRN, VLL, IES, and composite services. See the appropriate service management chapter for procedures that describe how to modify services from the topology view.

Managing OAM diagnostics from the topology view

A 5620 SAM operator can configure and execute OAM diagnostic tests from the service topology or composite service flat topology view. A right-click contextual menu of test types and test operations allows a GUI user to perform many test-management tasks. The OAM diagnostic functions on the map are enabled and disabled using a selector in the map window.

5620 SAM OAM diagnostic test management using the service topology map is supported for the following service types:

- VLAN, excluding 9500 MPR VLAN
- VLL Epipe
- VPLS
- VPRN

The 5620 SAM OAM diagnostic test management functions are also available for composite services using the composite service flat topology map.

You can use a contextual menu option to open a test-creation form for selected map objects such as NEs, SAPs, SDPs, MEPs, and MIPs. The form is automatically populated with the information for the selected objects. After you apply the test configuration, you can use the map to execute the test and view the results. A test result summary is viewable using statically displayed or mouse-over global info tables that are shown beside the object that initiates the test. By default, the info table for a tested object displays the five most recent test results; you can enable or disable the display of individual or all results.

The general OAM contextual menu options that are available include the following:

- Create OAM Tests—lists the tests that are appropriate for the service type and selected objects; choosing a test type opens the pre-populated test-creation form
- Select OAM Tests—opens a filterable list form from which you can choose previously created tests associated with one or two objects



Note — The tests that are listed using the Select OAM Tests option do not include generated tests, or manually added first-run or last-run tests in a test suite.

See Procedure 6-27 for information about enabling basic OAM-related map functions.

Working with Ethernet CFM objects

You can configure and manage Ethernet CFM objects such as MEGs, MEPs, and MIPs using the Ethernet CFM contextual menu option. MEPs and MIPs are represented iconically. For example, a SAP or SDP binding object can have a graphical connector to MEPs and MIPs, and a site object can be connected to a B-VPLS MEP.

Within a MEG, MEPs can be divided into logical groupings called sub-groups. A MEG which contains sub-groups is called a Global MEG. When created, a Global MEG has by default one subgroup.

A service topology map displays only one MEG at a time. The MEG is selectable using a drop-down list in the map window when the OAM function on the map is enabled. The CFM objects associated with the currently selected MEG are displayed.

For a MEP, the following attributes are displayed:

- the MEP level, as a number inside the icon
- the MEP direction, as the up or down direction in which the icon points
- the MEP administrative state, as the icon color
- the MEG sub-group to which the MEP belongs, as the icon outline color.



Note — For composite services, MEP generation does not occur for for VLAN uplinks and overlapping service sites.

When the Show Test Options check box is enabled, the roles assigned to MEPs for Test Suite Generation are displayed beside the MEP icons. The roles are Target, Source, and Hub or Spoke. See Procedure 6-27.

For a MIP, only the level is displayed.

The displayed Ethernet CFM contextual menu options for MEPs and MIPs depend on the Ethernet CFM configuration, for example, the MD level and whether MEPs and MIPs are already in the MEG.

When an operator right-clicks on the map background, the Ethernet CFM options are:

- global MEG creation, which opens a configuration form populated with the selected sites or all service sites, if none are selected.
- addition of a service to an existing global MEG

When the selected object is a SAP, you can create, view, change and delete MEPs. See Procedure 78-1 for information about configuring MEPs. You can enable, disable, and view MIPs. Enabling a MIP creates a MIP only when the configuration supports this function.

When the selected object is a VLAN uplink, a solid line is displayed between the two SAPs and an OAM icon is displayed above the port icons. Right-click on the OAM icon to display the following Ethernet CFM options:

- Edit MEP
- Delete MEP
- Disable MIP
- Change MEG Sub Group

When the selected object is an SDP binding, you can enable, disable, and view the associated MEPs.



Note — When you enable a MIP on a SAP or SDP binding, the 5620 SAM creates a MEG site if one does not exist, and uses explicit MHF creation.

6.4 Workflow to use 5620 SAM topology maps

1. Familiarize yourself with the components and basic operations of 5620 SAM maps. See sections 6.1 and 6.5 for more information.
2. Determine the map type you want to use. See section 6.2 for more information.
   - Select service maps to show which NEs are used by the services.
   - Select topology maps to show the relationship between NEs in a routing domain.
3. Configure map layout and object information tables. See section 6.6 for more information.
4. As required, create map filters to narrow the range of objects displayed. See section 6.6 for more information.
5. As required, create topology groups and populate the groups with devices to organize the network. See section 6.7 for more information.
6. As required, create physical links between managed and unmanaged devices to configure L1 management. See section 6.7 for more information.

6.5 Basic 5620 SAM topology map procedures

Use the following procedures to perform basic map management tasks.

Procedure 6-1 To open a map from the 5620 SAM main menu

1 Choose Application from the 5620 SAM main menu.

2 Choose a type of map to view from the menu options:

- Physical Topology to view Layer 1 network connectivity
- Service Tunnel Topology to view service tunnels
- Flat Maps→Physical Topology
- Flat Maps→Service Tunnel Topology
- EPS Path Topology

The appropriate map opens and displays the network objects.

See Procedure 6-7 for information about using the map elements. See Procedure 6-9 to list or view object information from a map. See section 6.1 for information about the map views.

Procedure 6-2 To open a service topology map

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Create an appropriate filter and click on the Search button. A list of services is displayed.

3 Select one or more services in the list and click on the Topology View button. A dialog box appears.

4 Click on the Yes button to continue. The Service Topology map opens.

See Procedure 6-7 for information about the map elements. See Procedure 6-9 to list or view object information from a map. See section 6.1 for information about the map views.

Procedure 6-3 To open an MPLS provisioned path map from the MPLS Path form

1 Choose Manage→MPLS→MPLS Paths from the 5620 SAM main menu. The Manage MPLS Paths form opens.

2 Create an appropriate filter and click on the Search button. A list of MPLS paths is displayed.

3 Select an MPLS path in the list and click on the Properties button. The MPLS Path configuration form for the MPLS path opens.

4 Click on the Provisioned Path tab. The hops of the MPLS path appear in a list.

5 Select a hop in the list and click on the Topology View button. The MPLS provisioned path map opens showing the hops between the devices.

See Procedure 6-7 for information about the map elements. See Procedure 6-9 to list or view object information from a map. See section 6.1 for information about the map views.

Procedure 6-4 To open a dynamic LSP path map from the LSP Path form

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form opens.

2 Create an appropriate filter and click on the Search button. A list of dynamic LSPs is displayed.

3 Select a dynamic LSP in the list and click on the Properties button. The Dynamic LSP (Edit) form opens.

4 Click on the LSP-Path Bindings tab. The LSP paths appear in a list.

5 Select an LSP path in the list and click on the Properties button. The LSP-Path Binding (Edit) form opens.

6 Perform one of the following:

a View the topology for provisioned paths:

i Click on the Provisioned Path tab. The hops of the LSP path appear in a list.

ii Select a hop in the list and click on the Topology View button. The LSP path map opens showing the hops between the devices.

b View the topology for actual paths:

i Click on the Actual Path tab. The hops of the actual path appear in a list.

ii Select a hop in the list and click on the Topology View button. The LSP path map opens showing the actual path hops between the devices.

c View the topology for CSPF paths:

i Click on the CSPF Path tab. The hops of the CSPF path appear in a list.

ii Select a hop in the list and click on the Topology View button. The LSP path map opens showing the CSPF path hops between the devices.

See Procedure 6-7 for information about the map elements. See Procedure 6-9 to list or view object information from a map. See section 6.1 for information about the map views.

Procedure 6-5 To open a flat map

1 Perform one of the following.

a Open a flat physical topology map.

i Choose Application→Flat Maps→Physical Topology from the 5620 SAM main menu. The Topology Filter - Physical Topology - Flat filter form opens.

ii Go to step 2.

b Open a service tunnel topology map.

i Choose Application→Flat Maps→Service Tunnel Topology from the 5620 SAM main menu. The Topology Filter - Service Tunnel Topology - Flat filter form opens.

ii Go to step 2.

See Procedure 6-7 for information about the map elements. See Procedure 6-9 to list or view object information from a map. See section 6.1 for information about the map views.

2 Perform one of the following:

a Perform Procedure 6-20 to create a filter definition.

b Perform Procedure 6-21 to load and apply a saved filter.

3 View the map.

4 Close the map.

Procedure 6-6 To open a dynamic LSP cross-connect topology map

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form opens.

2 Create an appropriate filter and click on the Search button. A list of dynamic LSPs is displayed.

3 Choose an LSP in the list and click on the Properties button. The Dynamic LSP (Edit) form opens.

4 Click on the Cross Connects tab. The cross-connects of the LSP path appear in a list.

5 Choose a cross-connect in the list and click on the Topology View button. The LSP path map opens and displays the cross-connects between the devices.

See Procedure 6-7 for information about the map elements. See Procedure 6-9 to list or view object information from a map. See section 6.1 for information about the map views.

Procedure 6-7 To view and understand map elements

1 Open a map, as described in Procedures 6-1 to 6-6.

2 View the map elements, which can include the following:

- device icons, which each display one of the following background colors to represent connectivity status and SNMP reachability
  - red—down or unreachable
  - yellow—resynchronizing or discovering
  - purple—management suspended
  - green—normal

  The icon in the top-right corner of a device icon represents the most serious alarm raised against the device.
  The icon in the middle right hand side of a device icon represents the alarm status for the device.

The icon in the bottom right corner of a device icon represents the connectivity to the device. During resynchronization, the icon represents the resynchronization status; for example, yellow.

- topology group icons, which have the following characteristics:
  - The background color white indicates that the topology group does not contain any descendant objects.
  - The color and icon in the upper left corner of the topology group icon indicate the most severe alarm on any of the devices in the group.
  - The color of the upper middle section of a topology group icon indicates the aggregated connectivity status of the devices in the group.
  - The color of the upper right corner of the topology group icon indicates the aggregated link status of the links in the group.

- composite service icons, which have the following characteristics:
  - The color and icon in the upper left corner of the composite service icon indicate the most severe alarm on any of the devices in the composite service.
  - The color of the upper middle section of the composite service icon indicates the aggregated connectivity status of the devices in the composite service.
  - The color of the upper right corner of the composite service icon indicates the aggregated link status of the links in the composite service.

- service tier icons in composite service maps, which have the following characteristics:
  - The color and icon in the upper left corner of the composite service icon indicate the most severe alarm on any of the devices in the service.
  - The color of the upper middle section of the composite service icon indicates the aggregated connectivity status of the devices in the service.
  - The color of the upper right corner of the composite service icon indicates the aggregated link status of the links in the service.

Procedure 6-8 To save a map to a file

You can use the Save to File button to save a portion of a map or the entire map to a file. You can save the file in JPEG, BMP or PNG format.

1 Open a map.

2 Click on the Save To File button. The save options are displayed in the drop-down menu.

3 Choose a type of view from the drop-down menu:

- Choose Save Map View to save the current view.
- Choose Save Full Map to save the entire map view.

The Save form opens.

4 Save the results.

i To choose a directory for the file, use the Save In parameter.

ii To create a filename, use the File Name parameter.

iii Choose BMP, JPEG, or PNG from the File of Type drop-down menu.

iv Click on the Save button. The map view is saved to the specified file.

Procedure 6-9 To view object information from a map

1 Open a map.

2 Right-click on one of the following objects:

- device icon
- plus sign icon in the centre of a link or link group
- port of a generic or unmanaged NE that indicates the endpoint of a link, path, tunnel, or service
- topology group icon

The appropriate contextual menu appears.

3 Choose a contextual menu option. The following are examples of the options available, depending on the type of object selected.

- Choose Properties to open the properties form for the object.
- Choose Scripts to open the properties form for an NE with the Scripts tab displayed.

Procedure 6-10 To manage the topology map window

The topology map panel and navigation tree panel are separated by a vertical split bar that you can use to control the panels. You can change the size, and hide, or show the map panel or the navigation tree panel.

1 To change the size of the map panel and the navigation tree panel, drag the vertical split bar to the left or right to control the amount of space used for the map panel and the navigation tree.

2 To hide the navigation tree panel, click on the vertical split bar left-facing arrow icon. The tree panel is hidden.

3 To show the map navigation tree panel, click on the vertical split bar right-facing arrow icon. The tree panel opens.

4 To hide the map panel, click on the vertical split bar right-facing arrow icon. The map panel is hidden.

5 To show the map panel, click on the vertical split bar left-facing arrow icon. The map panel opens.

Procedure 6-11 To zoom in and zoom out on a map

1 Open a map.

2 Perform one of the following:

- **a** Use the mouse wheel to zoom in and zoom out. Perform the following steps.
  - **i** Click on the map.
  - **ii** To zoom in, roll the mouse wheel forward.
  - **iii** To zoom out, roll the mouse wheel backward.
- **b** Use the Zoom In Tool and Zoom Out Tool. Perform the following steps.
  - **i** Click on the Zoom in Tool or Zoom out Tool button.
  - **ii** Move the mouse pointer into the map panel. The pointer changes to a magnifying glass containing a + or - sign.
  - **iii** Click on the area of the map you want to expand or contract. The map expands or contracts. Continue clicking until the desired zoom level is reached.
  - **iv** Use the opposite button and an equal number of clicks to return the map to its default setting.
  - **v** To return to the pointer icon, click on the Select Tool button in the toolbar.

3 Use the Scale combo box to specify a zoom level, and press ↵.

Procedure 6-12 To display only selected map objects

1 Open a map.

2 Select the objects.

3 Right-click on the selected objects and choose Show only Selected from the contextual menu. The map refreshes to display only the selected objects, and the word Hidden is displayed in the map panel to indicate that some objects are currently hidden.

4 To restore the previous map view, right-click in the map panel and choose Cancel Show Only from the contextual menu.

Procedure 6-13 To display only highlighted map objects

1 Open a map.

2 Click on the Legend button in the toolbar and choose Highlight Sessions from the drop-down menu. The Legend form opens with the Highlight Sessions tab displayed.

3 Select one or more highlight sessions in the list.

4 Right-click on the selected highlight sessions and choose Show Only Highlighted from the contextual menu. The map refreshes to display only the highlighted objects, and the word Hidden is displayed in the map panel to indicate that the non-highlighted objects are currently hidden.

5 To restore the previous map view, right-click in the map panel and choose Cancel Show Only from the contextual menu. The map refreshes to display the previous view.



Note — You can also restore the previous map view by right-clicking on the selected highlight sessions in the Legend form and choosing Cancel Show Only from the contextual menu.

6.6 5620 SAM topology map configuration procedures

Use the following procedures to perform map configuration tasks.

Procedure 6-14 To create an information table configuration

You can create an information table configuration for all map objects, selected map objects, or map highlights. See Procedure 6-15 to apply a configuration to all map objects. See Procedure 6-16 to apply a configuration to selected map objects. See Procedure 6-17 to apply a configuration to highlighted map objects.

1 Open a map.

2 Click on the Global Info Tables button. A drop-down menu opens with the information table configurations displayed.

3 Select the Configure menu item. The *topology_view* Info Table Configurations form opens.

4 Click on the Create button. The *topology_view* - Info Table Configuration form opens.

5 Configure the Configuration Name parameter.

6 For each map object type, click on the associated check box to select the attribute for display in the information table.



Note — If an applicable attribute is not selected for a specific object type, an information table is not displayed when you apply an information table configuration to objects of that type.

7 Click on the OK button. The *topology_view* - Info Table Configuration form closes, and the new configuration is listed on the *topology_view* - Info Table Configurations form.

8 Close the *topology_view* - Info Table Configurations form.

Procedure 6-15 To enable or disable a global information table

The Global Info Tables button allows you to view an information table for all map objects. An information table configuration must be created before it can be applied. See Procedure 6-14 for information about creating an information table configuration.

1 Open a map.

2 Click on the Global Info Tables button. A drop-down menu opens with the information table configurations displayed.

3 Perform one of the following:

a Select a radio button to apply an existing global information table configuration. The map is refreshed with the corresponding information table displayed beside the map objects.

b Click on the Off button. The global information table feature is disabled.

Procedure 6-16 To enable or disable a selected information table

The Selected Info Tables menu option allows you to view an information table for a map object, or a group of map objects. An information table configuration must be created before it can be applied to a map object or a group of map objects. See Procedure 6-14 for information about creating an information table configuration.

1 Open a map.

2 Right-click on a map object or a selection of map objects. A drop down menu opens.

3 Choose Selected Info Tables. A drop down menu opens with a list of information table configurations and an Off option.

4 Perform one of the following:

- **a** Choose an information table configuration. The map view is refreshed with the configured information table displayed beside the map objects.
- **b** Choose the Off option. The selected information tables for the selected map objects are no longer displayed.

Procedure 6-17 To re-enable or disable map highlights

1 Open the required map.

2 Click on the Legend button in the toolbar and choose Highlight Sessions from the drop-down menu. The Legend form opens with the Highlight Sessions tab displayed.

3 Perform one of the following:

- **a** Re-enable a disabled highlight. Perform the following steps.
  - **i** Select the check box in the Active column for the highlight.
  - **ii** Click on the Apply button. The map view is refreshed with the highlight displayed.
- **b** Disable the highlight. Perform the following steps.
  - **i** Deselect the check box in the Active column for the highlight.
  - **ii** Click on the Apply button. The map view is refreshed. The highlight and the associated information tables are no longer displayed.

4 Click on the Close button. The Legend - *topology* form closes.

Procedure 6-18 To enable or disable a highlight information table

You must create an information table configuration before you can apply the configuration to a map highlight. See Procedure 6-14 for information about creating an information table configuration.

1 Open the required map.

2 Click on the Legend button in the toolbar and choose Highlight Sessions from the drop-down menu. The Legend form opens with the Highlight Sessions tab displayed.

3 Select one or more highlight sessions in the list.

4 Right-click on the selected highlight sessions and choose Highlighted Info Sessions from the contextual menu. A drop-down menu opens with a list of information table configurations and an Off option.

5 Perform one of the following.

a Choose an information table configuration. The map view is refreshed with the specified information table displayed beside the highlighted map objects.

b Choose the Off option. The map view is refreshed and does not display information tables for the highlighted map objects.



Note — When a highlight is disabled or deleted, the map does not display the information tables that are associated with the highlight.

6 Click on the Close button. The Legend - *topology* form closes.

Procedure 6-19 To delete a map highlight

1 Open a map.

2 Click on the Legend button in the toolbar and choose Highlight Sessions from the drop-down menu. The Legend form opens with the Highlight Sessions tab displayed.

3 Click on a map highlight to select it.

4 Right-click on the selected highlight and choose Delete. A dialog box appears.

5 Click on the Yes button. The highlight is deleted.

6 Click on the Close button. The Legend - *topology* form closes.

Procedure 6-20 To create a map filter

Perform this procedure to configure a filter to restrict the objects in a map view. You can save the filter for searches on similar objects.

1 Open a map.

2 Click on the New Filter button. The Topology Filter - *topology_view* form opens.

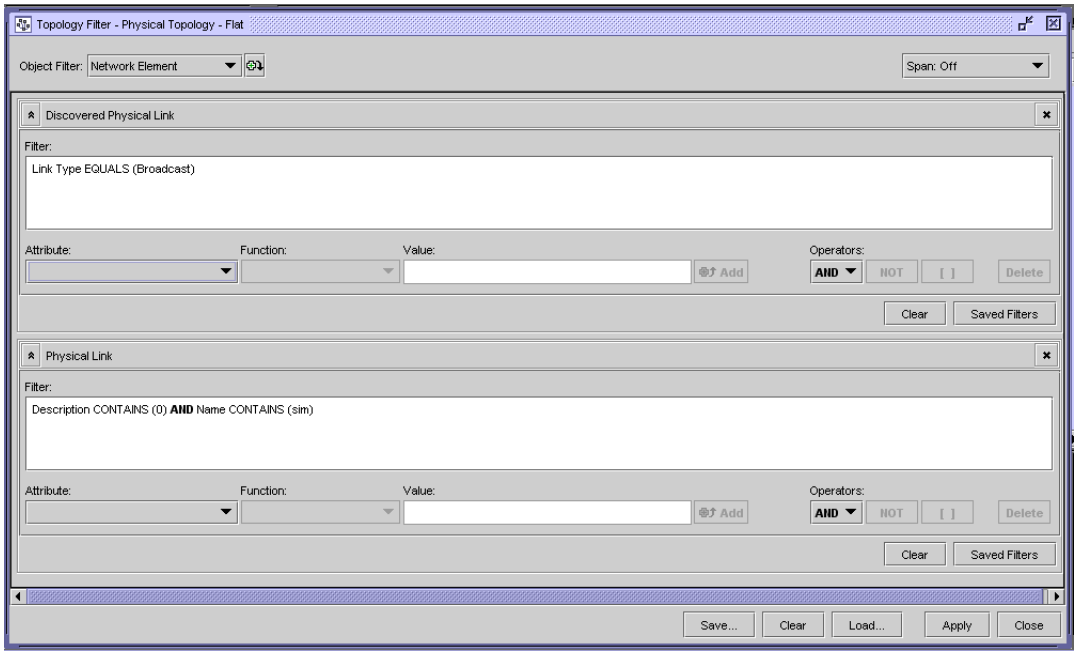
3 Choose an object filter from the Object Filter drop-down menu. Table 6-2 lists the filter options for each map type.

Table 6-2 Map filter options

Type of map	Filter options
Physical topology	Discovered Physical Link Network Element Optical Link Physical Link
Service tunnel topology	Network Element Tunnel

4 Click on the Add Object Filter button. The selected object filter is displayed in the filter panel as shown in Figure 6-15.

Figure 6-15 Map filter



5 Choose one or more of the object filters to create the filter. See chapter 3 for information about creating filters.

6 Configure the Span parameter.

7 Perform one of the following:

a Click on the Apply button to apply the filter and not save the filter. The map view is refreshed to display only the map objects defined in the filter. The filter selector displays Filter Applied.

b Perform the following steps to save the filter.

i Click on the Save button. The Save Filter form opens.

ii Configure the parameters:

- Filter Name
- Description
- Public

8 Click on the Save button. The Save Filter form closes.

9 Close the Topology Filter - *topology_view* form.

Procedure 6-21 To load and apply a saved filter to a topology map

See Procedure 6-20 for information about creating a filter definition tree.

1 Open a map.

2 Click on the saved filter selector and choose a filter from the drop-down list.

The 5620 SAM applies the filter and the map view is refreshed to display only the map objects specified in the filter. The filter name is displayed in the saved filter selector.

Procedure 6-22 To auto-layout icons on a map



Caution — After you click on the Auto-Layout button and confirm the action, the existing map layout is overwritten and cannot be recovered.

1 Open a map.

2 Perform one of the following:

a Auto-layout all of the icons on the map.

i Click on the Auto-Layout Tool button and choose one of the following options:

- Circular - emphasizes ring and star topologies in networks. Objects are grouped according to the network structure and arranged in circles or radial tree structures.
- Smart Organic - emphasizes inherent data groupings and symmetries. This information helps with understanding the interconnections of complex structures.
- Endpoint Layout (VPLS, VLL, mirror, and composite service sites only) - all endpoints are snapped close to the associated parent site.

A dialog box appears.

ii Click on the Yes button.

b Auto-layout a group of icons on the map.

i Select multiple objects.

ii Right-click on an object in the group, choose Layout Selected, and choose one of the following options from the contextual menu:

- Circular
- Smart Organic
- Endpoint Layout (VPLS, VLL, mirror, and composite service sites only)

A dialog box appears.

iii Click on the Yes button.

The map layout changes so that icons with links between them are closer together, and icons without links between them are moved to the periphery.

Procedure 6-23 To search for a specific network object

1 Open a map.

2 Perform one of the following:

a To search for a network object by typing the name, or part of the name of the network object:

i Click on the Find button in the map toolbar.

ii Choose Find Vertex or Find Link. The Find *object* form opens.

iii Configure the filter criteria and click on the Search button. A list of objects is displayed.



Note — The search function is case sensitive.

iv Select an object in the list.

b To search for a network object by pasting the name of the network object from the clipboard:

i Click on the network object that you want to locate from the equipment view of the navigation tree or from a generated or displayed list.

ii Click on the Copy to Clipboard icon to copy the network object name to the clipboard.

iii Click on the Find button.

iv Choose Find Vertex or Find Link. The Find Object form opens.

v Click on the Paste button. The network object that you copied to the clipboard is displayed in the Find object with label containing text field.



Note — Only the first item listed on the clipboard is pasted in the Find object with label containing text field of the Find Object form.

c Use the Quick-search field on the map window. Perform the following steps.

i Type part or all of the object name in the Quick-search field beside the toolbar icons.

ii Press ↵. The map shifts to display the first object that matches the search criterion.

iii Press F3 to shift the map focus to the next matching object, if the search finds multiple matches.

iv Press CTRL-F3 to shift the map focus to the previous matching object, if the search finds multiple matches.

v Go to step 5.

3 Click on the OK button.

a If a match is found, the map panel displays the topology group that contains the object and the map navigation tree expands to display the group. If necessary, the map panel scrolls to the portion of the map where the object is displayed.

b If multiple matches are found, the Find Object form opens with a drop-down list of all of the search results. Go to step 4.

4 Select a network object and click on the OK button. The map panel displays the topology group that contains the object and the map navigation tree expands to display the group. If necessary, the map panel scrolls to the portion of the map where the object is displayed.

5 Manage the object, as required.

Procedure 6-24 To create a bookmark

See section 6.1 for more information about the bookmark function.

1 Open a map.

2 Locate the topology group that you want to bookmark.



Note — Bookmarks are associated with a map view. To use the bookmark after it is created, you must be in the same view where you created the bookmark or a view that shares the same group, for example, a topology group that belongs to both the physical topology map and the service tunnel map.

3 Click on the Bookmarks button and choose Add Bookmark. A bookmark for the currently displayed topology group is created.

Procedure 6-25 To manage bookmarks

See section 6.1 for more information about the bookmark function.

1 Open a map, as described in Procedures 6-1 to 6-6.



Note — Bookmarks are associated with a map view. To use the bookmark after it is created, you must be in the same view where you created the bookmark or a view that shares the same group, for example, a topology group that belongs to both the physical topology map and the service tunnel map.

Bookmarks that were not created in the map view currently displayed, or that are invalid, are disabled and cannot be selected. In the Manage Bookmarks form, these bookmarks appear in italics.

2 Click on the Bookmarks button and choose Manage Bookmarks. The Manage Bookmarks form opens.

3 Perform one of the following:

a Create a top-level folder to manage the bookmarks.

i Click on the New Folder button. The Folder Properties form opens.

ii Enter the name of the new folder in the Name field and click on the OK button. A new top-level folder is added to the list panel.

b Create a folder in an existing folder.

i Select an existing folder in the list panel and click on the New Folder button. The Folder Properties form opens.

ii Enter the name of the new folder in the Name field and click on the OK button. A new folder is added to the list panel inside the existing folder.

c Organize your bookmarks and folders. Drag and drop bookmarks and folders in and out of other folders in the list panel.

d Rename a bookmark or folder.

i Select an existing bookmark or folder in the list panel and click on the Rename button. The Rename form opens with the existing name in the Name field.

ii Change the text in the Name field and click on the OK button. The name of the bookmark or folder is modified.

e Delete a bookmark or folder.

i Select a bookmark or folder that you want to delete in the list panel.

ii Click on the Delete button. The selected bookmark or folder is removed from the list panel and the bookmark drop-down menu on the map toolbar.

4 Click on the Close button to close the Manage Bookmarks form and save the changes.

Procedure 6-26 To change the map background image

To view the map background image examples provided by the 5620 SAM, navigate to the background directory in the 5620 SAM client Installation directory, for example, /nms/images/map/background.

When adding your own map image to the directory, ensure that the file type is GIF and that the size is a maximum of 2000 × 2000 pixels.

The default background image is defaultBackgroundImage.gif.

1 Open a map, as described in Procedures 6-1 to 6-6.

2 In the map navigation tree, right-click on the topology group for which you want to change the map background image and choose Properties from the contextual menu. The Group - Network (Edit) form opens.

3 Modify the Background Image parameter to specify a new map image file, for example, n_america.gif.

4 Click on the OK button. A dialog box appears.

5 Click on the Yes button to proceed. The background image for the topology group changes to the selected image.

6.7 5620 SAM topology map management procedures

Use the following procedures to perform map management tasks.

Procedure 6-27 To use OAM diagnostic functions on service topology and composite service flat topology maps

Perform this procedure to enable the OAM diagnostic functions on a service topology or composite service flat topology map, and use the basic OAM controls in the map window. See the other procedures in this chapter for information about using specific elements such as the toolbar buttons and info tables.

1 Create a service topology map by selecting the service in the Manage Services form and clicking on the Topology View button.

2 Select the OAM check box at the bottom left of the map window.

3 To manage one or more objects, select the objects and right-click on the set of objects to choose an option from the contextual menu.

4 To select a MEG to display, choose the MEG from the drop-down list of available MEGs at the bottom of the map window.



Note — You can also create a MEG directly from the topology map by right-clicking on an empty portion of the map to open a contextual menu. Select Ethernet CFM→Create Global MEG. Refer to Procedure 32-5 for detailed information.

5 To view the properties of the selected MEG, click on the MEG Properties button at the bottom of the window. The Global Maintenance Entity Group (Edit) form opens with the General tab displayed. The service displayed on the map is listed on the Service tab.

6 To resynchronize the MIPs in the selected MEG, click on the Resync MIPs button at the bottom of the window.

7 To display the Test Generation Options for MEPs in the selected MEG, enable the Show Test Options check box at the bottom of the map window. See "Working with Ethernet CFM objects" in section 6.3.

8 Use the other procedures in this chapter to refine the map contents or display object properties, as required.

9 Use the right-click contextual menu options to configure and manage OAM objects, as required. See "Managing OAM diagnostics from the topology view" in section 6.1 for a functional description of the available contextual menu options for OAM diagnostics.

Procedure 6-28 To create a topology group



Note — A topology group can contain a maximum of 500 NEs.

1 Open the Group (Create) form using one of the following methods.

   a Choose Create→Equipment→Group from the 5620 SAM main menu.

   b Right-click on the Network icon in the equipment view of the navigation tree and choose Equipment→Create Group from the contextual menu.

2 Configure the parameters:

   - Group Name
   - Description
   - Background Image

3 Click on the Apply button.

4 Click on the Spans tab.

5 Click on the Add button. The Select Span(s) - Equipment Group form opens with a list of available spans.

6 Select one or more spans to apply to the topology group.

7 Click on the OK button. The Select Span(s) - Equipment Group form closes and a dialog box appears.

8 Click on the OK button to confirm the action.

   After the topology group is created, an object for the topology group is displayed in the equipment navigation tree, and on the appropriate topology maps.

Procedure 6-29 To populate a topology group



Note — A topology group can contain a maximum of 500 NEs.

1 Choose Application→Physical Topology, or Service Tunnel Topology from the 5620 SAM main menu. The appropriate map window opens.

2 Populate topology groups, as required,

a Click on a map object in the map panel, for example, a router or router group, and drag the object onto the topology group object to which you want the map object to belong in the:

- map panel
- map navigation tree

The map object becomes a descendant object of the topology group.

b Click on a topology group object in the map navigation tree and drag the object onto another group object in the map navigation tree to which you want the group object to belong. The topology group object becomes a descendant object of another group object.

Procedure 6-30 To modify a topology group and create topology groups with the same parameter settings

1 Right-click on the topology group object on the map for which you want to modify the parameters and choose Properties from the contextual menu. The Group (Edit) form opens.

2 Modify the parameters as required.

3 Click on the Apply button. A dialog box appears.

4 Click on the Yes button to save the changes.

5 If required, click on the Copy button to create more topology groups based on the same parameter information. A Group (Create) form opens with the existing parameter information.

6 Edit the parameter information as required.

7 Click on the OK button. The Group (Create) form closes.

8 Close the Group (Edit) form.

Any changes to the properties of a topology group appear immediately on the equipment navigation tree and the appropriate topology maps.

Procedure 6-31 To delete a topology group

When you delete a topology group object, the topology group cannot contain any devices or descendant topology groups.

1 Choose Application→Physical Topology, or Service Tunnel Topology from the 5620 SAM main menu. The appropriate map window opens.

2 Drag and drop all devices and descendant topology groups from the topology group that you want to delete to another topology group or the root group, for example, the network.

3 Right-click on the topology group object that you want to delete on the map and choose Delete from the contextual menu. A dialog box appears.

4 Click on the Yes button to proceed. The topology group is deleted.

Procedure 6-32 To modify a service or composite service using the topology view

You can use the service topology or composite service flat topology view to add, modify, or navigate to service components. The service configuration form can also be accessed directly at any time from this view by right-clicking any component. This allows quick access to conduct more detailed component configuration.

1 Perform one of the following.

   a Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

   b Choose Manage→Service→Composite Services from the 5620 SAM main menu. The Manage Composite Services form opens.

2 Configure a search filter, if required, and click on the Search button. A list of services or composite services is displayed.

3 Perform one of the following.

   a Select a service and click on the Topology View button. The Service Topology map opens.

   b Select a composite service and click on the Flat Topology View button. The Composite Service Flat Topology View map opens.

4 Right-click on the map background, or on one or more selected service sites, or individual components (for example, a SAP) to display a contextual menu of configuration options. When you choose an option, a configuration form opens. If you choose to create an OAM test, the appropriate test configuration form opens.

5 See the appropriate service management chapter for information about modifying a specific service type or Chapter 32 for information on performing OAM diagnostic tests.

Procedure 6-33 To create a physical link

The MDA type for both physical link endpoints must be the same. Only one physical link can be configured on a port.

Users with Device Mgmt privileges can create, modify, and delete physical links.

1 Open the Physical Link (Create) form using one of the following methods.

   a Choose Create→Equipment→Create Physical Link from the 5620 SAM main menu.

   b Right-click on the topology map background in the equipment view of the navigation tree and choose Equipment→Physical Link from the contextual menu.

2 Configure the parameters:

- Name
- Description
- Endpoint A Type
- Endpoint B Type
- Notes

3 Configure the parameters in the Endpoint A panel by performing one of the following.

   a If you set the Endpoint A Type parameter in step 2 to Port, go to step 4.

   b If you set the Endpoint A Type parameter in step 2 to Network Element, go to step 5.

   c If you set the Endpoint A Type parameter in step 2 to LAG, go to step 6.

4 Configure the parameters in the Endpoint A - Port panel by performing one of the following steps.

a Use the Select Endpoint A - Port - Physical Link form to search for a port.

i Click on the Select button in the Endpoint A – Port panel to choose a managed endpoint for the physical link. The Select Endpoint A - Port - Physical Link form opens.

ii Use the configurable filter and click on the Search button to generate a list of ports.

iii Select a port and click on the OK button. The Select Endpoint A - Port - Physical Link form closes and the port parameter information is displayed in the Endpoint A - Port panel of the Physical Link (Create) form.

b Choose a port from the equipment navigation tree.

i Select a port object and click on the Copy to Clipboard button. The port information is copied to the clipboard.

ii Click on the Paste from Clipboard button in the Endpoint A - Port panel of the Physical Link (Create) form. The port parameter information is displayed in the Endpoint A - Port panel.

5 Configure the parameters in the Endpoint A - Network Element panel by performing one of the following steps.

a Use the Select Endpoint A - Network Element - Physical Link form to search for a port.

i Click on the Select button in the Endpoint A panel to choose a managed endpoint for the physical link. The Select Endpoint A - Network Element - Physical Link form opens.

ii Use the configurable filter and click on the Search button to generate a list of NEs.

iii Select an NE and click on the OK button. The Select Endpoint A - Network Element - Physical Link form closes and the NE parameter information is displayed in the Endpoint A - Network Element panel of the Physical Link (Create) form.

b Choose an NE from the equipment navigation tree:

i Select an NE and click on the Copy to Clipboard button. The NE information is copied to the clipboard.

ii Click on the Paste from Clipboard button in the Endpoint A - Network Element panel of the Physical Link (Create) form. The NE parameter information is displayed in the Endpoint A - Network Element panel.

6 Configure the parameters in the Endpoint A - LAG panel by performing one of the following steps.

a Use the Select Endpoint A - LAG - Physical Link form to search for a port.

i Click on the Select button in the Endpoint A panel to choose a managed endpoint for the physical link. The Select Endpoint A - LAG - Physical Link form opens.

ii Use the configurable filter and click on the Search button to generate a list of NEs.

iii Select an NE and click on the OK button. The Select Endpoint A - LAG - Physical Link form closes and the NE parameter information is displayed in the Endpoint A - LAG panel of the Physical Link (Create) form.

b Choose an NE from the equipment navigation tree:

i Select an NE and click on the Copy to Clipboard button. The NE information is copied to the clipboard.

ii Click on the Paste from Clipboard button in the Endpoint A - LAG panel of the Physical Link (Create) form. The NE parameter information is displayed in the Endpoint A - LAG panel.

7 Configure the parameters in the Endpoint B panel by performing one of the following.

a If you set the Endpoint B Type parameter in step 2 to Port, go to step 8.

b If you set the Endpoint B Type parameter in step 2 to Network Element, go to step 9.

c If you set the Endpoint B Type parameter in step 2 to Unmanaged NE, go to step 11.

d If you set the Endpoint B Type parameter in step 2 to LAG, go to step 12.

8 Configure the parameters in the Endpoint B - Port panel by performing one of the following.

a Use the Select Endpoint B - Port - Physical Link form to search for a port.

i Click on the Select button in the Endpoint B panel to choose a managed endpoint for the physical link. The Select Endpoint B - Port - Physical Link form opens.

ii Use the configurable filter and click on the Search button to generate a list of ports.

iii Select a port and click on the OK button. The Select Endpoint B - Port - Physical Link form closes and the port parameter information is displayed in the Endpoint B - Port panel of the Physical Link (Create) form.

b Choose a port from the equipment navigation tree.

i Select a port object and click on the Copy to Clipboard button. The port information is copied to the clipboard.

ii Click on the Paste from Clipboard button in the Endpoint B - Port panel of the Physical Link (Create) form. The port parameter information is displayed in the Endpoint B - Port panel.

9 Configure the parameters in the Endpoint B - Network Element panel by performing one of the following.

a Use the Select Endpoint B - Network Element - Physical Link form to search for a port.

i Click on the Select button to choose a managed endpoint for the physical link. The Select Endpoint B - Network Element - Physical Link form opens.

ii Use the configurable filter and click on the Search button to generate a list of NEs.

iii Select an NE and click on the OK button. The Select Endpoint B - Network Element - Physical Link form closes and the NE parameter information is displayed in the Endpoint B - Network Element panel of the Physical Link (Create) form.

b Choose an NE from the equipment navigation tree:

i Select an NE and click on the Copy to Clipboard button. The NE information is copied to the clipboard.

ii Click on the Paste from Clipboard button in the Endpoint B - Network Element panel of the Physical Link (Create) form. The NE parameter information is displayed in the Endpoint B - Network Element panel.

10 If the Endpoint B is an unmanaged NE that the 5620 SAM recognizes as an unmanaged mobile NE such as an eNodeB, go to step 14.

11 Configure the parameters in the Endpoint B - Unmanaged NE panel:

- Unmanaged - Name
- Unmanaged - Management Address
- Unmanaged - Description



Note — If the 5620 SAM is to manage endpoint B, configure the Unmanaged - Name parameter with the management IP address of the unmanaged NE.

When the 5620 SAM discovers the NE, the unmanaged endpoint of the physical link is updated with the newly managed NE on the topology map.

12 Configure the parameters in the Endpoint B - LAG panel by performing one of the following.

a Use the Select Endpoint B - LAG - Physical Link form to search for a port.

i Click on the Select button in the Endpoint B panel to choose a managed endpoint for the physical link. The Select Endpoint B - LAG - Physical Link form opens.

ii Use the configurable filter and click on the Search button to generate a list of ports.

iii Select a port and click on the OK button. The Select Endpoint B - LAG - Physical Link form closes and the port parameter information is displayed in the Endpoint B - LAG panel of the Physical Link (Create) form.

b Choose a port from the equipment navigation tree.

i Select a port object and click on the Copy to Clipboard button. The port information is copied to the clipboard.

ii Click on the Paste from Clipboard button in the Endpoint B - LAG panel of the Physical Link (Create) form. The port parameter information is displayed in the Endpoint B - Port panel.

13 Go to step 17.

14 Click on the Select button in the Endpoint B - Unmanaged NE (LTE) panel to choose an unmanaged mobile NE such as an eNodeB. The Select Unmanaged NE - Physical Link form opens.

15 Use the configurable filter and click on the Search button to generate a list of unmanaged mobile NEs for example, eNodeB devices.

16 Select an unmanaged mobile NE and click on the OK button. The Select Unmanaged NE - Physical Link form closes and the NE information is displayed in the Endpoint B - Unmanaged NE (LTE) panel of the Physical Link (Create) form.

17 Click on the OK button to close the form. The physical link is created between the two endpoints and can be viewed from the physical topology map.

Procedure 6-34 To modify a physical link and create physical links with the same parameter settings

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Physical Link from the object drop-down list.

3 Configure the filter criteria and click on the Search button.

4 Select a physical link in the list and click on the Properties button. The Physical Link (Edit) form opens.

5 Modify the parameters as required.

6 Click on the Apply button to save the changes.

7 If required, click on the Copy button to create more physical links based on the same parameter information. If the Copy button is not visible, click on the More Actions button and choose Copy. A Physical Link (Create) form opens with the existing parameter information.

8 Edit the parameter information as required.

9 Click on the OK button. The Physical Link (Create) form closes.

10 Close the Physical Link (Edit) form.

After a physical link is created, you can view the link on the physical topology map.

Procedure 6-35 To manage link referencing

You can select one or more links to manage link referencing.

1 Select the links. Hold down the shift key and right-click the links to be managed.

2 Hold down the shift key and right-click on the topology map background in the equipment view of the of the navigation tree and choose Reference from the contextual menu. Choose from one of the following options.

   a To reference the links that you have chosen, choose Reference Selected Discovered Links.

   b To clear the references, choose Clear Reference for All Selected Links.

   c To clean up references (removing the Reference for links that are down), choose Cleanup Selected Discovered Links.



Note 1 — If you select no links, right-clicking on the topology map background will give you the following options (in the Reference contextual menu):

- Reference All Discovered Links in NE Group (in which case, References will be created only for links in the open/active topology group).
- Clear Reference for All Discovered Links in NE Group
- Cleanup All Discovered Links in NE Group

Note 2 — You can also reference links and clear references using the Discovered Link Property form (for a single link) and the Manage Equipment form (for multiple links). See Procedure 6-38.

Procedure 6-36 To delete a physical link

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Physical Link from the object drop-down list.

3 Configure the filter criteria and click on the Search button.

4 Select a physical link in the list and click on the Delete button. A dialog box appears.

5 Click on the Yes button to proceed. The physical link is deleted.



Note — When a NE is unmanaged or removed, all the physical links that terminate on the ports or on the NE itself are deleted.

Procedure 6-37 To configure bandwidth availability on physical links

Use this procedure to configure bandwidth parameters on links being used by service CAC.



Note — This capability is only available if service CAC has been configured. See "To configure service CAC to automatically bind PBB tunnels" in the *5620 SAM System Administrator Guide*.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Perform one of the following.

   a Choose Discovered Physical Link from the object drop-down menu.

   b Choose Physical Link from the object drop-down menu.

3 Configure the filter criteria and click on the Search button.

4 Select a physical link in the list and click on the Properties button. The Physical Link (Edit) form opens.

5 Click on the Bandwidth tab.

6 Select the Endpoint A or the Endpoint B tab.

7 Configure the following endpoint bandwidth parameters:

- Bandwidth (%)
- Used Bandwidth (Mbps)
- Utilization Threshold (%)

8 Configure the following effective bandwidth parameters:

- Name
- Bandwidth (Mbps)
- Booking Factor (%)
- Utilization Threshold (%)
- Used Bandwidth (Mbps)

9 To view a summary of bandwidth usage for all tunnels and services currently using the physical link, click on the Bandwidth Usage tab.

10 Click on the OK button. The Physical Link (Edit) form closes.

11 Close the Manage Equipment form.

Procedure 6-38 To view and modify discovered physical link properties

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Discovered Physical Link from the object drop-down list.

3 Configure the filter criteria, if required, and click on the Search button.

4 Select a discovered physical link in the list and click on the Properties button. The Discovered Physical Link (Edit) form opens with the General tab displayed.

5 Configure the following parameters, if required:

- Name
- Description

6 Perform one of the following to configure the link reference information, if required.

a Click on the Reference Discovered Links button. If the Reference Discovered Links button is not visible, click on the More Actions button and choose Reference Discovered Links. The parameters in the Reference panel are populated with reference information.

b Click on the Clear Reference button. If the Clear Reference button is not visible, click on the More Actions button and choose Clear Reference. The parameters in the Reference panel are reset.

7 Select the appropriate tab to view other information, as required.

8 Click on the OK button. The Discovered Physical Link (Edit) form closes.

9 Close the Manage Equipment form.

Procedure 6-39 To switch from a backup/standby protected link to an in-service protected link on a 9500 MPR device

1 In the Physical topology map, right-click on the protected link between two 9500 MPR NEs which is indicated in blue, and select Expand Group. The links expand to show the backup/standby link in blue, and the in-service link in green.

2 To switch the standby/backup link to in-service and the in-service link to backup/standby, right-click on the relevant port or card and select Properties. The Physical Port (Edit) form opens.

3 Click on the Protection tab. From the Equipment Protection Scheme parameter and the Receiver Protection Scheme parameter, select the Commands option.

4 Click on the Apply button. A dialog box appears.

5 Click on the Yes button. The Physical Port (Edit) form closes.

7 — 5620 SAM scheduling

7.1 Scheduling overview *7-2*

7.2 Workflow to manage scheduling *7-4*

7.3 Scheduling procedures *7-5*

7.1 Scheduling overview

The 5620 SAM scheduling functions allow the creation of 5620 SAM-based schedules for the automatic execution of tasks at designated times.

You can associate a schedule that you create using the 5620 SAM with a task that supports scheduling. A task such as running an STM test suite can be immediately processed, scheduled for later execution, or retained for future use. A task that is associated with a schedule is called a scheduled task. A scheduled task must be created in the configuration form for the task. For example a STM test suite scheduled task must be created in the STM test suite configuration form. After scheduled tasks are created they are associated with a schedule.

A 5620 SAM schedule is configurable for one-time or ongoing task execution. You can optionally specify the time at which an ongoing schedule is to stop functioning.

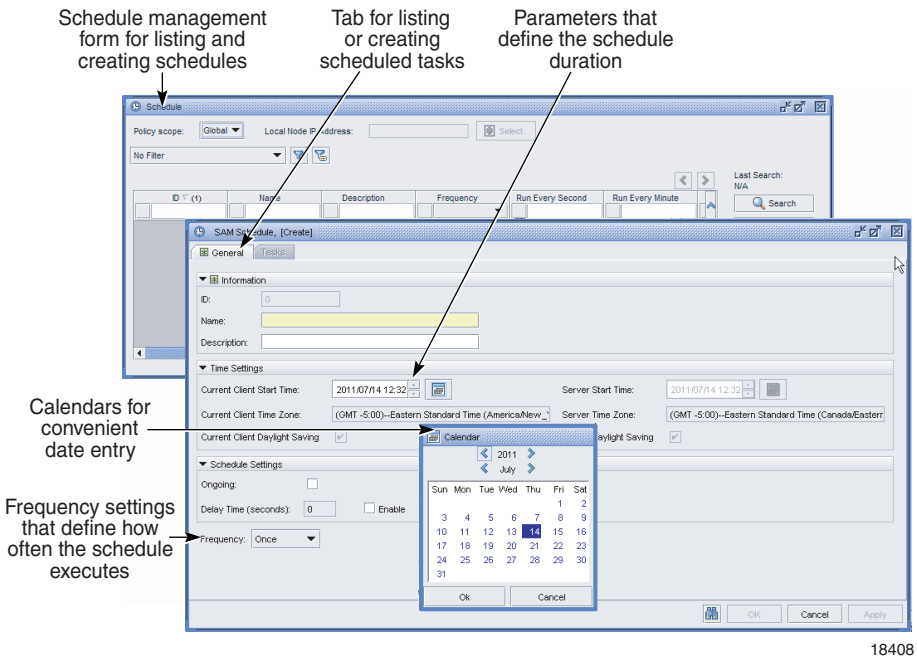
To simplify creating 5620 SAM-based schedules when the user and server are in different time zones, the 5620 SAM converts and displays schedule times specific to the user and server. For example, if a user in Ottawa wants to schedule a task on a 5620 SAM server in London, the 5620 SAM calculates the time difference and displays the user and server local times.

User time zones are configured in the user preferences form. If a time zone is not configured on the main server, the 5620 SAM uses the default time zone on the single-user client or client delegate server station, If the default time zone is not one of the 5620 SAM time zone options, the 5620 SAM displays the time zone ID and uses the UTC value without the time zone offset.

The 5620 SAM displays whether daylight saving time is in effect for the client and the server. Daylight saving time is specified for the user start time and is based on the client time zone. Daylight saving time does not specify the current time and end time.

Figure 7-1 shows the Schedule management form and the SAM Schedule configuration form.

Figure 7-1 Schedule management and configuration forms



SAM schedules

A SAM schedule exists only in the 5620 SAM and is not deployed to the target NEs. When a configured SAM schedule run time arrives, the 5620 SAM executes the associated task and compiles the task results for presentation to 5620 SAM clients.

A delay time for executing SAM scheduled runs can be configured to delay the execution of a run within a scheduled task in cases when a previously scheduled run is still executing. The 5620 SAM attempts to execute the new run at the configured delay time; if the run cannot execute at the delay time, the 5620 SAM skips the scheduled run. When a previous run completes and the next scheduled run is triggered, the run executes and is not delayed, whether a delay time is configured.

The SAM schedule functionality in the 5620 SAM uses the 5620 SAM server time zone to trigger the scheduled tasks.

A 5620 SAM-based schedule supports the following tasks:

- STM test suites. See chapter 77 for more information about STM test suites.
- NE software upgrades. See “NE maintenance overview” in the *5620 SAM System Administrator Guide* for more information about NE software upgrades.

Consider the following when you create a SAM schedule or a scheduled task.

- Ensure that scheduled tasks are run sufficiently far apart to allow one task to finish before the next starts. Otherwise, the next occurrence of the task is skipped or delayed, if the delay time is configured.
- Do not create schedules that overlap, as no validation is performed to ensure that a newly configured schedule does not overlap with an existing schedule.

- A new SAM scheduled task is shut down by default and must be turned up before it can be executed with one exception. Scheduled software upgrade tasks associated with all NE types are by default auto-enabled.
- Users with write access permissions to a specific schedule package can view or delete all the created schedules and scheduled tasks related to the package. Other users can only view schedules. See "5620 SAM user security tasks" in the *5620 SAM System Administrator Guide* for more information about user permissions.
- By default, the 5620 SAM associates a scheduled task with the user account that is used to create the scheduled task. You can assign a different user account to a scheduled task. The user account must have the assigned scope of command role that is appropriate for the task, or the 5620 SAM does not execute the scheduled task.
- When you create a scheduled task that runs on a daily, weekly, or monthly schedule, you must reset the scheduled task when daylight savings time is in effect. See Procedure 7-8 for information about resetting schedules.
- If a schedule is not synchronized with the server time, you must reset the scheduled task. See Procedure 7-8 for information about resetting schedules
- SAM schedules are not distributed to the target NEs.
- You cannot delete a schedule that has a dependency, for example, one that is associated with a task.
- One minute is added to the default start and end time values of a 5620 SAM-based schedule to allow time for schedule configuration.
- A monthly SAM schedule with the Run Every Month or Run Every Months parameter configured uses a 30-day interval.
- When you create a monthly SAM schedule using the Run Every parameter and specify a date that does not exist for the specified months, the last date of the month is used. For example, if you create a monthly scheduled task, starting January 31st, the scheduled task will run on February 28th, March 31st and April 30th when those months are specified in the schedule.

7.2 Workflow to manage scheduling

1. Create a task, such as an STM test suite, that supports the 5620 SAM scheduling function.
2. Create or modify a SAM schedule. See Procedure 7-1 for more information.
3. Associate a task with the schedule. See Procedure 7-2 or 7-3 for more information.
4. For a SAM scheduled task that requires user account privileges other than the default privileges, assign a different user account to the scheduled task. See Procedure 7-4 for more information.
5. Turn up the scheduled task. See Procedure 7-5 for more information.

6 After the schedule executes the task, review the current status of the SAM scheduled task. See Procedure 7-6 for more information.

7 As required, perform one of the following.

a execute the scheduled task immediately; see Procedure 7-7 for more information

b reset the scheduled task; see Procedure 7-8 for more information

c delete the scheduled task; see Procedure 7-9 for more information

d delete the schedule; see Procedure 7-10 for more information

7.3 Scheduling procedures

Use the following procedures to manage 5620 SAM schedules and scheduled tasks.

Procedure 7-1 To configure a SAM schedule

1 Choose Tools→Schedules→Schedule from the 5620 SAM main menu. The Schedule form opens.

2 Perform one of the following:

a To create a schedule, click on the Create button. The SAM Schedule (Create) form opens with the General tab displayed.

b To configure an existing schedule, perform the following steps.

i Choose SAM Schedule from the object drop-down list.

ii Configure the filter criteria. A list of schedules is displayed.

iii Select an entry in the list and click on the Properties button. The SAM Schedule (Edit) form opens with the General tab displayed.



Note 1 — You can modify a schedule only when you are logged in as the user who is assigned to the schedule. To assign a different user account to the schedule, perform Procedure 7-4.

Note 2 — You cannot modify a schedule that is in use by a scheduled task.

3 Configure the parameters:

- Name
- Description
- Current Client Start Time
- Current Client End Time
- Ongoing
- Delay Time (seconds)
- Enable
- Frequency

The Current Client End Time parameter is configurable when the Ongoing parameter is disabled and the Frequency parameter value is set to a value other than Once.



Note — If you are creating a schedule to apply to policy audits, the Frequency parameter must be set to a value greater than 15 minutes.

When a SAM Schedule is not Ongoing and is assigned to a task, the 5620 SAM raises an alarm when the Current Client End Time expires.

4 Perform one of the following that corresponds to the Frequency parameter value that is specified in step 3:

a When the parameter is set to Once, go to step 5.

b When the parameter is set to Per Second, configure the following parameters:

- Run Every Second
- Run Every Seconds

c When the parameter is set to Per Minute, configure the following parameters:

- Run Every Minute
- Run Every Minutes

d When the parameter is set to Per Hour, configure the following parameters:

- Run Every Hour
- Run Every Hours

e When the parameter is set to Per Day, configure the following parameters:

- Run Every Day
- Run Every Days
- Run Every

f When the parameter is set to Per Week, configure the following parameters:

- Run Every Week
- Run Every Weeks
- Run Every

The Run Every parameter is not configurable when the Ongoing parameter is enabled.

g When the parameter is set to Per Month, configure the following parameters:

- Run Every Month
- Run Every Months
- Run Every

The Run Every parameter is not configurable when the Ongoing parameter is enabled.

5 Click on the OK button to save the changes. The SAM Schedule (Create) form closes and the Schedule form reappears.

6 Close the Schedule form.

Procedure 7-2 To associate a task with a 5620 SAM schedule

1 Perform one of the following.

a Assign a SAM schedule to a task.

i Open the properties form for a task that supports SAM schedules, such as an STM test suite.

ii Click on the Schedule button. The *task_name* (Edit) form opens, go to step 2.

b View scheduled tasks associated with a SAM schedule.

i Choose Tools→Schedules→Schedule from the 5620 SAM main menu. The Schedule form opens.

ii Choose SAM Schedule (Schedule) from the object drop-down list.

iii Configure the filter criteria. Click on the Search button. A list of SAM schedules is displayed.

iv Select a SAM schedule in the list and click on the Properties button. The SAM Schedule (Edit) form opens.

v Click on the Tasks tab button. A list of scheduled tasks appears.

vi Choose a task from the list. Click on the Properties button to view the scheduled tasks.

2 Configure the parameters:

- Scheduled Task Name
- Scheduled Task Description
- Administrative State



Note — When you set the Administrative State parameter to Enabled, the scheduled task goes into effect, according to the schedule parameters. Ensure that the task is appropriately configured before you set the parameter to Enabled.

3 Click on the Select button to choose a schedule. The Select Schedule - STM Scheduled Task *task_name* form opens with a list of schedules.

Note — The form lists only the schedules that are associated with the current 5620 SAM user.

4 Select a schedule in the list and click on the OK button. The Select Schedule - STM Scheduled Task *task_name* form closes and the scheduled task is displayed on the STM Scheduled Task (Create) form.

5 Click on the OK button. The STM Scheduled Task (Create) form closes.

6 Close the SAM Schedule (Edit) or task properties form.

7 Close the Schedule form if the form is open.

Procedure 7-3 To modify a scheduled task

Note — You can modify a SAM scheduled task only when you are logged in as the user who is assigned to the SAM scheduled task. To assign a different user account to the SAM scheduled task, perform Procedure 7-4.

1 Choose Tools→Schedules→Scheduled Task from the 5620 SAM main menu. The Scheduled Task form opens.

2 Choose SAM Scheduled Task from the object drop-down list.

3 Configure the filter criteria. A list of scheduled tasks is displayed.

4 Select a scheduled task in the list and click on the Properties button. The scheduled task (Edit) form opens.

5 Modify the parameters, as required.

6 Click on the OK button. The SAM Scheduled Task (Edit) form closes and the Scheduled Task form reappears.

7 Close the Scheduled Task form.

Procedure 7-4 To assign a different user account to a SAM scheduled task

Perform this procedure to associate a SAM scheduled task with a different user account. By default, the 5620 SAM associates a scheduled task with the user account that is active when the SAM scheduled task is created.



Note — The 5620 SAM does not execute a SAM scheduled task unless the scheduled task is associated with an existing 5620 SAM user account. If you delete the user account that is associated with a SAM scheduled task, you must assign a different user account to the SAM scheduled task. Only a 5620 SAM user with an assigned administrator scope of command role can assign a user account to a SAM scheduled task.

1. Choose Tools→Schedules→Scheduled Task from the 5620 SAM main menu. The Scheduled Task list form opens.
2. Choose SAM Scheduled Task (schedule) from the object drop-down list.
3. Configure the filter criteria. A list of SAM scheduled tasks is displayed.
4. Select a scheduled task and click on the Reassign User button. A dialog box informs you that the new user must have the appropriate access permissions to manage the scheduled task. See "5620 SAM user security tasks" in the *5620 SAM System Administrator Guide* for information about scope of command roles and access permissions.
5. Set the Change Current User To parameter.
6. Click on the OK button.

Procedure 7-5 To turn up or shut down a scheduled task

1. Choose Tools→Schedules→Scheduled Task from the 5620 SAM main menu. The Scheduled Task form opens.
2. Choose SAM Scheduled Task (Schedule) from the object drop-down list.
3. Configure the filter criteria. A list of scheduled tasks is displayed.
4. Select an entry in the list and click on the Task Action button.
5. Choose one of the following from the menu that appears:
   a. Turn Up—enable the scheduled task. The administrative state changes to enabled.
   b. Shut Down—disable the scheduled task. The administrative state changes to disabled.
6. Close the Scheduled Task form.

Procedure 7-6 To view the current status of a SAM scheduled task

1 Choose Tools→Schedules→Scheduled Task from the 5620 SAM main menu. The Scheduled Task form opens.

2 Choose SAM Scheduled Task from the object drop-down list.

3 Configure the filter criteria. A list of SAM scheduled tasks is displayed.

4 Select a SAM scheduled task in the list.

5 Click on the Task Action button and choose View Result from the menu that appears.

6 View the Execution Status indicator. The value is one of the following:

- None
- In Progress
- Skip Requested
- Skipped
- Stop Requested
- Stopped
- Succeeded
- Failed
- Delay Requested
- Delayed
- Started

7 View the Status indicator. The value is one of the following:

- Running—The scheduled task is running.
- Not Running—The scheduled task is not running.
- Completed—The scheduled task execution completed successfully.

8 Close the Scheduled Task form.

Procedure 7-7 To execute a SAM scheduled task

1 Turn up the SAM scheduled task, as described in Procedure 7-5.

2 Choose Tools→Schedules→Scheduled Task from the 5620 SAM main menu. The Scheduled Task form opens.

3 Choose SAM Scheduled Task from the object drop-down list.

4 Configure the filter criteria. A list of SAM scheduled tasks is displayed.

5 Select an entry and click on the Task Action button.

6 Choose Execute from the menu that appears. The 5620 SAM executes the SAM scheduled task.

7 Close the Scheduled Task form.

8 Perform Procedure 7-6 to view the SAM scheduled task execution status, if required.

Procedure 7-8 To reset a scheduled task

1 Choose Tools→Schedules→Scheduled Task from the 5620 SAM main menu. The Scheduled Task form opens.

2 Choose SAM Scheduled Task from the object drop-down list.

3 Configure the filter criteria to list tasks that the administrative state is enabled, and click on the Search button. A list of scheduled tasks is displayed.

4 Select a scheduled task in the list.

5 Click on the Task Action button and choose Shut Down from the menu that appears. The Turn Up button is enabled.

6 Click on the Task Action button and choose Turn Up from the menu that appears. The Shut Down button is enabled.

7 Close the Scheduled Task form.

Procedure 7-9 To delete a scheduled task



Note — You can delete a SAM scheduled task only when you are logged in as the user who is assigned to the SAM scheduled task. To assign a different user account to the SAM scheduled task, perform Procedure 7-4.

1 Choose Tools→Schedules→Scheduled Task from the 5620 SAM main menu. The Scheduled Task form opens.

2 Choose SAM Scheduled Task from the object drop-down list.

3 Configure the filter criteria. A list of scheduled tasks is displayed.

4 Select a scheduled task in the list.

5 Click on the Task Action button and choose Shut Down from the menu that appears. The Delete button is enabled.

6 Click on the Delete button. A dialog box appears.

7 Click on the Yes button. The 5620 SAM deletes the scheduled task.

8 Close the Scheduled Task form.

Procedure 7-10 To delete a schedule



Note 1 — You cannot remove a schedule that is associated with a scheduled task; you must first delete the scheduled task.

Note 2 — You can delete a SAM scheduled task only when you are logged in as the user who is assigned to the SAM scheduled task. To assign a different user account to the SAM scheduled task, perform Procedure 7-4.

1 Perform Procedure 7-9 to delete the scheduled tasks associated with the schedule.

2 Choose Tools→Schedules→Schedule from the 5620 SAM main menu. The Schedule form opens.

3 Choose SAM Scheduled from the object drop-down list.

4 Configure the filter criteria. A list of schedules is displayed.

5 Select a schedule in the list and click on the Delete button. A dialog box appears.

6 Click on the Yes button. The 5620 SAM deletes the schedule.

7 Close the Schedule form.

Device management

8 — Device support

9 — Device commissioning and management

10 — Device discovery

11 — Device CLI sessions

12 — Working with network objects

13 — Device object configuration

14 — Logical group object configuration

15 — Shelf object configuration

16 — Port and channel object configuration

17 — Inventory management

18 — Card migration

19 — TCA

20 — Bulk operations

21 — Auto-provision

8 — Device support

8.1 Device support overview *8-3*

8.2 Workflow to prepare 5620 SAM to manage devices *8-4*

8.3 1830 PSS support *8-6*

8.4 5780 DSC support *8-6*

8.5 7210 SAS support *8-6*

8.6 Workflow to manage 7210 SAS devices *8-10*

8.7 7450 ESS support *8-13*

8.8 Workflow to manage 7450 ESS devices *8-13*

8.9 7705 SAR support *8-16*

8.10 Workflow to manage 7705 SAR devices *8-22*

8.11 7710 SR support *8-25*

8.12 Workflow to manage 7710 SR devices *8-25*

8.13 7750 MG support *8-28*

8.14 7750 SR support *8-28*

8.15 Workflow to manage 7750 SR devices *8-29*

8.16 7950 XRS support ***8-32***

8.17 Workflow to manage 7950 XRS devices ***8-34***

8.18 9471 WMM support ***8-37***

8.19 9500 MPR and 9500 MPRe support ***8-37***

8.20 eNodeB support ***8-38***

8.21 OmniSwitch support ***8-38***

8.22 Workflow to manage OmniSwitch devices ***8-43***

8.23 GNE support ***8-46***

8.24 Workflow to manage GNEs ***8-49***

8.1 Device support overview

The 5620 SAM can manage the following Alcatel-Lucent devices:

- 1830 PSS-1
- 1830 PSS-4
- 1830 PSS-16
- 1830 PSS-32
- 1830 PSS-32s
- 5780 DSC
- 7210 SAS-D 6F 4T
- 7210 SAS-D 6F 4T ETR
- 7210 SAS-E
- 7210 SAS-M 24F
- 7210 SAS-M 24F 2XFP
- 7210 SAS-M 24F 2XFP ETR
- 7210 SAS-T
- 7210 SAS-T ETR
- 7210 SAS-X 24F 2XFP
- 7450 ESS
- 7705 SAR
- 7710 SR
- 7750 MG
- 7750 SR
- 7750 SR-c4
- 7750 SR-c12
- 7750 SR-12E
- 7950 XRS-20
- 7950 XRS-16c
- 9471 WMM
- 9500 MPR
- 9500 MPRe
- eNodeB
- OS 6250M
- OS 6250SME
- OS 6400
- OS 6450
- OS 6850
- OS 6855
- OS 6900
- OS 9600
- OS 9700
- OS 9700E
- OS 9800
- OS 9800E
- OS 10K

The 5620 SAM also provides limited management support for generic NEs, which are typically non-Alcatel-Lucent devices using SNMP.

For core-network devices such as the 7450 ESS, 7710 SR, and 7750 SR, the 5620 SAM supports the current software release and the three immediately previous major releases. For example, a 5620 SAM, Release 11.0 system can manage a 7750 SR, Release 11.0, 10.0, 9.0, or 8.0. Older device releases are not supported.

For devices other than core-network devices, the 5620 SAM release support varies. See the *5620 SAM Network Element Compatibility Guide* for specific device support information.



Caution — When a device introduces a maintenance release, you must ensure that your 5620 SAM software supports the new device release before you upgrade the device to the new release. You may need to upgrade the 5620 SAM to support the new device release. See the *5620 SAM Network Element Compatibility Guide* for more information.

The 5620 SAM GUI displays a device feature or function only if the device supports the feature or function. The 5620 SAM user documentation describes the major variations in support, including device-specific procedures for specific implementations, but does not describe the following minor GUI variations for different devices:

- partial support for the parameter list on a form
- partial support for the buttons and tabs on a form

The following documents describe 5620 SAM support for specific device releases:

- *5620 SAM Network Element Compatibility Guide*—lists the device releases and functions that the 5620 SAM supports
- *5620 SAM Parameter Guide*—lists and describes the supported parameters; includes device-specific variations in parameter defaults and ranges

See the device user documentation for information about device functions, parameters, and CLI commands that are outside the scope of the 5620 SAM documentation. Contact Alcatel-Lucent technical support for specific network or facility considerations.



Note 1 — You can use an OSS client to configure many of the functions available on the 5620 SAM GUI. See "Communication with the 5620 SAM server" in the *5620 SAM XML OSS Interface Developer Guide* for information about using an OSS client.

Note 2 — You can use 5620 SAM scripts and templates to configure managed devices. See "Script and template management" in the *5620 SAM Scripts and Templates Developer Guide* for more information.

Device-specific workflows

The *5620 SAM User Guide* describes the management of many devices; however 5620 SAM management of some devices, for example, optical and LTE devices, is described in other guides. Each device-specific section in this chapter contains one of the following:

- if the information is contained in the *5620 SAM User Guide*, a workflow in this chapter describes the high-level steps that are required to manage the device, including how to:
  - commission and discover the device
  - configure and manage device objects
  - configure and manage the policies and services associated with the device
- a reference to the guide that describes 5620 SAM management of the device

8.2 Workflow to prepare 5620 SAM to manage devices

The following workflow describes the high-level steps that are required to prepare the 5620 SAM to perform network management. This workflow is common to all 5620 SAM-managed devices.

This workflow and the device-specific workflows in this chapter assume that you have performed the following prerequisite tasks:

- installed the 5620 SAM software, as described in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*
- installed the physical device as per the appropriate device-specific hardware user documentation
- integrated the 5620 SAM with other Alcatel-Lucent products, such as the 5650 CPAM or another third-party product, if required. See the *5620 SAM Integration Guide* for information.

1 Review the 5620 SAM GUI functionality in order to view, configure, and manage the device.

a Perform basic GUI operations to allow you to perform device, network, policy, and service management functions, create custom workspaces, customize user preferences, and perform GUI search functions; see chapter 3.

b Manage equipment using the equipment navigation tree; see chapter 5.

c Manage equipment using topology maps; see chapter 6.

d Perform 5620 SAM scheduling functions as required, to allow the automatic execution of tasks at designated times; see chapter 7.

2 Perform all required 5620 SAM and UNIX security management tasks for accessing and securing the managed device. See “NE user and device security” in the *5620 SAM System Administrator Guide* for more information.

i Implement the user security measures required to protect all 5620 SAM data, software, and hardware, and monitor the system and network for any security threats.

ii Set up all required 5620 SAM user accounts and user groups with the required scope of command roles, span of control permissions, and the ongoing monitoring and management of those accounts. As required, review the 5620 SAM permissions, access levels, and descriptions of all pre-defined scope of command roles and profiles.

3 Perform advanced configuration tasks on the 5620 SAM as required, to meet your specific operational requirements for managing the device. See “5620 SAM Advanced configuration tasks” in the *5620 SAM System Administrator Guide* for information.

a Configure, maintain, and administer the 5620 SAM operational environment including software and license components, system components, network functions, and system preferences.

b Perform the required tasks to maintain 5620 SAM system redundancy, and as required, monitor or perform any maintenance activity switching or switchovers.

c Use the 5620 SAM database manager to view, configure, and monitor the 5620 SAM database, which contains the managed device configurations.

4 Review the 5620 SAM support for the device; see this chapter and the *5620 SAM Network Element Compatibility Guide*.

5 Proceed to the device-specific workflows in this chapter to determine which functions can be performed on the device, and then configure the functions.

8.3 1830 PSS support

The 1830 Photonic Service Switch product family provides CWDM, DWDM, and OTN capabilities. Photonic networking increases flexibility and operational automation. The 5620 SAM supports the following 1830 PSS devices:

- 1830 PSS-1 - edge aggregation device; the supported variants are the following:
  - 1830 PSS-1 AHP amplifier
  - 1830 PSS-1 GBE edge devices
  - 1830 PSS-1 MD4H edge device
- 1830 PSS-4 - edge device
- 1830 PSS-16 - end office device
- 1830 PSS-32 - central office device
- 1830 PSS-32s - client-line device

The following documents describe 5620 SAM management and configuration of the 1830 PSS:

- *5620 SAM User Guide*—Describes management of optical devices which does not differ from other network elements
- *5620 SAM Optical User Guide*—Describes 1830 PSS discovery, configuration, and management using the 5620 SAM
- *5620 SAM Optical Parameter Reference*—Provides a list of all optical device parameters that the 5620 SAM supports

8.4 5780 DSC support

The 5620 SAM allows you to view the properties for the equipment, instance, Diameter proxy agent, and policy charging rules for the 5780 DSC. The 5780 DSC is represented in the 5620 SAM equipment navigation tree. The instance, Diameter proxy agent, and policy charging rule properties are viewable using the Manage→Mobile Core→DSC Instances 5620 SAM main menu option.

The *5620 SAM LTE EPC User Guide* describes 5780 DSC discovery and management using the 5620 SAM.

8.5 7210 SAS support

This section describes the 5620 SAM support for Alcatel-Lucent 7210 SAS devices.

7210 SAS-D support

The 7210 SAS-D is an intelligent Ethernet edge-demarcation device that extends enhanced Carrier Ethernet VPN service delivery to the CE. The license for a 7210 SAS-D is based on the chassis type. The 5620 SAM supports the following chassis types:

- 7210 SAS-D 6F 4T
- 7210 SAS-D 6F 4T ETR



Note — The 5620 SAM supports only access mode for 7210 SAS-D 6F 4T ETR ports.

7210 SAS-E support

The 7210 SAS-E is a Carrier Ethernet CE device that is typically owned and managed by a customer. Using software based on the 7750 SR OS and managed by the 5620 SAM, the 7210 SAS-E extends Carrier Ethernet VPN services to the CE. The 7210 SAS-E can also be deployed as an aggregation device for smaller sites.

7210 SAS-E daughter cards

The 7210 SAS-E supports an integrated 2 × 12-Gig IOM card on a single chassis. The equipment navigation tree displays a card slot with one daughter card that contains 12 × 100/1000 Ethernet SFP ports and 12 × 10/100/1000 Ethernet ports.

7210 SAS-M and 7210 SAS-X support

The 7210 SAS-M is a CE device that provides MPLS-enabled metropolitan and WAN Carrier Ethernet service delivery, Ethernet-based mobile backhaul, and residential service access.

The 7210 SAS-X is an MPLS-enabled Ethernet aggregation device for small and medium-sized networks that provides business, mobile backhaul, and residential services. It is similar to the 7210 SAS-M, but has 10Gb/s uplink ports, enhanced traffic management, greater scalability, and hierarchical QoS functions.

The 5620 SAM supports the following 7210 SAS-M and 7210 SAS-X chassis types:

- 7210 SAS-M 24F
- 7210 SAS-M 24F 2XFP
- 7210 SAS-M 24F 2XFP ETR
- 7210 SAS-X 24F 2XFP



Note — If you use the CLI or BOF to change the mode of a 7210 SAS-M from Access Uplink to Network, or from Network to Access Uplink, you must unmanage and remanage the device. The mode is shown on the Uplink Mode tab of the shelf properties form.

7210 SAS-T support

The 7210 SAS-T is an Ethernet access device that provides demarcation for services managed to the customer edge and Ethernet aggregation in smaller network locations. The 7210 SAS-T is equipped with the following ports:

- 12 × 10/100/1000 Ethernet SFP
- 10 × 10/100/1000Base-TX copper
- 4 × 10GigE XFP

Ports can be configured in access or uplink mode.

The 5620 SAM supports the following chassis variants:

- 7210 SAS-T 12F 10T 4XFP
- 7210 SAS-T 12F 10T 4XFP ETR

The 7210 SAS-T ETR supports Power over Ethernet (PoE) connections on ports 19, 20, 21, and 22. See Procedure 16-18 for more information.

System resource profile

The 5620 SAM supports system resource allocation on 7210 SAS devices using the system resource profile. You can configure system resources to suit your network requirements by assigning more resources to functions that are used extensively, and fewer resources to functions that are used less. Unused functions can be disabled, and their resources made available for other functions. Not all functional areas are configurable for all devices. System resource profile functional areas and applicable devices are listed in Table 8-1.

Table 8-1 System resource profile

Function	Applicable NE chassis
G8032 fast flood	7210 SAS-M, Release 4.0 R6 or later, in network mode only
SAP ingress internal ACL	7210 SAS-D, Release 5.0 R1 or later 7210 SAS-M and 7210 SAS-X, Release 4.0 R6 or later 7210 SAS-T, Release 6.0 R2 or later
SAP egress internal ACL	7210 SAS-D, 7210 SAS-M and 7210 SAS-X, Release 5.0 R1 or later 7210 SAS-T, Release 6.0 R2 or later
SAP ingress QoS	7210 SAS-D, 7210 SAS-E, 7210 SAS-M, and 7210 SAS-X, Release 5.0 R1 or later 7210 SAS-T, Release 6.0 R2 or later
Queues	7210 SAS-X, Release 5.0 R4 or later
Router	7210 SAS-M (in network mode), Release 6.0 R1 or later 7210 SAS-X, Release 6.0 R1 or later
Ethernet CFM	7210 SAS-D, Release 5.0 R1 or later 7210 SAS-M, Release 4.0 R6 or later 7210 SAS-T, Release 6.0 R2 or later



Note — Configuration changes for G8032 fast flood, Queues, and Router are boot-time enabled, and take effect during the next NE reboot. Changes to all other functions are run-time enabled and take effect immediately, if sufficient resources are available.

System resources are allocated in units called chunks. The number of chunks and the chunk size vary by device chassis. Table 8-2 lists the chunk size for each chassis type.

Table 8-2 System Resources

NE chassis	Chunk size (# of entries)	Total available chunks
7210 SAS-D	512	See the device scaling guide or your Alcatel-Lucent technical support representative for more information.
7210 SAS-E	256	
7210 SAS-M	512	
7210 SAS-T	512	
7210 SAS-X	512	

Resources are allocated by assigning a value from the applicable range. A value of 0 disables the function. The sum of resources allocated must not exceed the total available resources for the system. If you assign more than the allocated number of chunks, functions are disabled.

For ACL and QoS functions, configuring system resources is accomplished in two steps. First, divide overall system resources among the main functional areas: SAP ingress internal ACL, SAP egress internal ACL, and SAP ingress QoS. Second, allocate the resources specified for each functional area to the criteria within that function, such as MAC, IPv4, and 64 or 128-bit IPv4/v6. The total number of chunks assigned to the criteria must not exceed the number of chunks allocated to the function. When you specify a value of MAX, the system allocates resources as required on a first come, first served basis, up to the available limit.

See Procedure 13-20 and the 7210 SAS documentation for more information about system resource allocation.

8.6 Workflow to manage 7210 SAS devices

The following workflow describes the sequence of high-level tasks required to commission, configure, and manage 7210 SAS NEs and services. This workflow assumes that the physical devices have been installed.The management functions are supplemental to the general management functions described in section 8.2.

1. Determine configuration requirements for the installed device; see this chapter, the *5620 SAM Network Element Compatibility Guide*, and the *5620 SAM Parameter Guide* for device specific information.
2. Commission the device for 5620 SAM management; see chapter 9 for more information. Configure polling policies as described in Procedure 9-5.
3. Perform 5620 SAM discovery of the commissioned network devices, and optionally configure SSH2 security for CLI sessions; see chapter 10 for more information.
4. As required, manage and configure equipment; see chapter 12 for more information about equipment management and configuration. Additionally, configure the following:
   - **a** split horizon groups as described in Procedure 16-16
   - **b** LAGs as described in Procedures 14-10 and 14-11
   - **c** frame-based accounting as described in Procedure 13-19
   - **d** system resource profile as described in Procedure 13-20
   - **e** dry contact sensors as described in Procedure 15-3
   - **f** channelized TDM ports as described in Procedure 16-14
5. Create security policies and management access filters for NEs, and create NE user accounts that provide secure NE access using RADIUS or TACACS+ authentication. See “NE user and device security” in the *5620 SAM System Administrator Guide* for more information.
6. If required, perform NE maintenance functions such as backing up and restoring device configurations, upgrading device software, and monitoring deployment of configuration changes to devices. See “NE maintenance” in the *5620 SAM System Administrator Guide* for more information.

7 Create equipment inventories of managed devices; see chapter 17 for more information.

8 As required, perform additional device management functions such as the following:

- **a** TCP enhanced authentication between NEs. See “TCP enhanced authentication” in the *5620 SAM System Administrator Guide* for more information
- **b** threshold-crossing alarms; see chapter 19 for more information
- **c** bulk configuration changes; see chapter 20 for more information
- **d** automatic provisioning; see chapter 21 for more information

9 Configure NE routing and forwarding; see chapter 22 for general routing and forwarding information. As required, configure specific routing and forwarding functions such as the following:

- **a** NE protocols; see chapter 23 for more information.
- **b** MPLS and LSPs; see chapter 25 for more information.
- **c** service tunnels to carry service traffic; see chapter 27 for more information.
- **d** Lawful Intercept; see chapter 28 for more information
- **e** IPsec; see chapter 29 for more information
- **f** 5620 SAM alarm policies; see chapter 31 for more information
- **g** OAM diagnostic tests; see chapter 32 for more information

10 As required, configure redundancy in the managed network using functions such as the following:

- **a** VRRP; see chapter 33 for more information
- **b** APS; see chapter 34 for more information
- **c** MC peer groups; see chapter 36 for more information
- **d** MC endpoint groups; see chapter 38 for more information
- **e** MC LAG groups; see chapter 39 for more information
- **f** MC synchronization groups; see chapter 40 for more information
- **g** MC ring groups; see chapter 41 for more information

11 Create 5620 SAM policies that define the conditions for 5620 SAM management functions; see chapter 42 for general information about 5620 SAM policy management. As required, configure specific policy types such as the following:

- **a** QoS policies; see chapter 43 and Procedures 43-2, 43-4, 43-5, 43-7, 43-9, 43-11, 43-13, 43-19, and 43-27 for more information
- **b** multicast policies; see chapter 45 for more information

c time of day policies; see chapter 46 for more information

d VRRP policies; see chapter 47 for more information

e auto tunnels policies; see chapter 48 for more information

f 802.1x policies; see chapter 50 for more information

g PBB MRP policies; see chapter 51 for more information

h connection profile policies; see chapter 53 for more information

i service PW template policies; see chapter 73 for more information

j residential subscriber policies; see chapter 54 for more information

k remote network monitoring policies; see chapter 55 for more information

l constraint policies; see chapter 56 for more information

m NAT policies; see chapter 57 for more information

n format and range policies; see chapter 58 for more information

12 Configure services and related functions; see chapters 61 and 62 for general service information. As required, configure specific services and related functions such as the following:

a virtual ports; see chapter 63 for more information

b customers; see chapter 64 for more information

c residential subscribers of customer services; see chapter 65 for more information

d VLL Epipe services as described in Procedure 67-1

e VLL Cpipe services to provide point-to-point connectivity between customer access ports; see chapter 67 for more information

f VPLS to provide virtual LAN connectivity that connects multiple customer sites in a bridged domain as described in Procedure 68-7. See chapter 68 for more information.

g mirror services for troubleshooting customer traffic issues or for use with Lawful Intercept; see chapter 69 for more information

h IES to provide an IP interface between customer traffic and the Internet; see chapter 70 for more information

i composite services to connect various types of services; see chapter 74 for more information

j 5620 SAM schedules and scheduled tasks to automate 5620 SAM service management functions such as running OAM diagnostics; see chapter 7 for more information

k OAM diagnostic tests into suites of manual and automatically-generated tests using the Service Test Manager; see chapter 77 for more information

l Ethernet Connectivity Fault Management; see chapter 78 for more information

m RCA audit; see chapter 80 for more information

8.7 7450 ESS support

The Alcatel-Lucent 7450 Ethernet Service Switch supports service-aware Ethernet aggregation across IP/MPLS-based networks, providing VPLS, VLL and advanced IP services. The 7450 ESS supports a wide range of interfaces.

A Network Domain feature allows users to determine which network ports are eligible to transport traffic of individual SDPs. This information is used for the SAP-ingress queue allocation algorithm applied to VPLS SAPs. See chapter 22 for more information.

The 5620 SAM provides network management functions for the 7450 ESS.

The 7450 ESS OAM toolkit includes ITU-TY.1731 with Synthetic Loss Measurement (SLM), IEEE 802.1ag, IEEE 802.3ah, Ethernet local management interface (E-LMI), VPLS OAM and service mirroring. This toolkit is also integrated into the 5620 SAM.

8.8 Workflow to manage 7450 ESS devices

The following workflow describes the sequence of high-level tasks required to commission, configure, and manage 7450 ESS NEs and services. This workflow assumes that the physical devices have been installed. The management functions are supplemental to the general management functions described in section 8.2.

1 Determine configuration requirements for the installed device; see this chapter, the *5620 SAM Network Element Compatibility Guide*, and the *5620 SAM Parameter Guide* for device specific information.

2 Commission the device for 5620 SAM management; see chapter 9 for more information. Configure polling policies as described in Procedure 9-4.

3 Perform 5620 SAM discovery of the commissioned network devices, and optionally configure SSH2 security for CLI sessions; see chapter 10 for more information.

4 As required, manage and configure equipment; see chapter 12 for more information about equipment management and configuration. Additionally, configure the following:

a mixed mode as described in Procedure 15-6

b IEEE 1588 PTP clock as described in Procedures 15-14 and 15-15

5 Create security policies and management access filters for NEs, and create NE user accounts that provide secure NE access using RADIUS or TACACS+ authentication. See “NE user and device security” in the *5620 SAM System Administrator Guide* for more information.

6 If required, perform NE maintenance functions such as backing up and restoring device configurations, upgrading device software, and monitoring deployment of configuration changes to devices. See “NE maintenance” in the *5620 SAM System Administrator Guide* for more information.

7 Create equipment inventories of managed devices; see chapter 17 for more information.

8 As required, perform additional device management functions such as the following:

- **a** TCP enhanced authentication between NEs. See “TCP enhanced authentication” in the *5620 SAM System Administrator Guide* for more information
- **b** card migration; see chapter 18 for more information
- **c** threshold-crossing alarms; see chapter 19 for more information
- **d** bulk configuration changes; see chapter 20 for more information
- **e** automatic provisioning; see chapter 21 for more information

9 Configure NE routing and forwarding; see chapter 22 for general routing and forwarding information. As required, configure specific routing and forwarding functions such as the following:

- **a** NE protocols; see chapter 23 for more information
- **b** MPLS and LSPs; see chapter 25 for more information
- **c** service tunnels to carry service traffic; see chapter 27 for more information
- **d** Lawful Intercept; see chapter 28 for more information
- **e** IPsec; see chapter 29 for more information
- **f** ISA-Video; see chapter 30 for more information
- **g** 5620 SAM alarm policies; see chapter 31 for more information
- **h** OAM diagnostic tests; see chapter 32 for more information

10 As required, configure redundancy in the managed network using functions such as the following:

- **a** VRRP; see chapter 33 for more information
- **b** APS; see chapter 34 for more information
- **c** MC peer groups; see chapter 36 for more information
- **d** MC endpoint groups; see chapter 38 for more information
- **e** MC LAG groups; see chapter 39 for more information
- **f** MC synchronization groups; see chapter 40 for more information
- **g** MC ring groups; see chapter 41 for more information

11 Create 5620 SAM policies that define the conditions for 5620 SAM management functions; see chapter 42 for general information about 5620 SAM policy management. As required, configure specific policy types such as the following:

- **a** QoS policies; see chapter 43 for more information
- **b** filter policies; see chapter 44 for more information
- **c** multicast policies; see chapter 45 for more information
- **d** time of day policies; see chapter 46 for more information
- **e** VRRP policies; see chapter 47 for more information
- **f** auto tunnels policies; see chapter 48 for more information
- **g** RADIUS-based accounting policies; see chapter 49 for more information
- **h** 802.1x policies; see chapter 50 for more information
- **i** PBB MRP policies; see chapter 51 for more information
- **j** connection profile policies; see chapter 53 for more information
- **k** service PW template policies; see chapter 73 for more information
- **l** residential subscriber policies; see chapter 54 for more information
- **m** remote network monitoring policies; see chapter 55 for more information
- **n** constraint policies; see chapter 56 for more information
- **o** NAT policies; see chapter 57 for more information
- **p** format and range policies; see chapter 58 for more information

12 Configure services and related functions; see chapters 61 and 62 for general service information. As required, configure specific services and related functions such as the following:

- **a** virtual ports; see chapter 63 for more information
- **b** customers; see chapter 64 for more information
- **c** residential subscribers of customer services; see chapter 65 for more information
- **d** VLL Apipe, Cpipe, Epipe, Fpipe, and Ipipe services to provide point-to-point connectivity between customer access ports; see chapter 67 for more information
- **e** VPLS to provide virtual LAN connectivity that connects multiple customer sites in a bridged domain; see chapter 68 for more information
- **f** mirror services for troubleshooting customer traffic issues or for use with Lawful Intercept; see chapter 69 for more information
- **g** IES to provide an IP interface between customer traffic and the Internet; see chapter 70 for more information

h VPRN services to provides a virtual IP network that connects multiple customer sites; see chapter 71 for more information

i composite services to connect various types of services; see chapter 74 for more information

j Application Assurance to provide deep-packet inspection and application-based subscriber traffic management; see chapter 76 for more information

k 5620 SAM schedules and scheduled tasks to automate 5620 SAM service management functions such as running OAM diagnostics; see chapter 7 for more information

l OAM diagnostic tests into suites of manual and automatically-generated tests using the Service Test Manager; see chapter 77 for more information

m Ethernet Connectivity Fault Management; see chapter 78 for more information

n RCA audit; see chapter 80 for more information

8.9 7705 SAR support

The 7705 SAR is an IP/MPLS aggregation and mobile backhaul router for the mobile RAN. Located at cell sites, the 7705 SAR uses PW over MPLS to aggregate mobile 2G and 3G traffic that it backhauls to the core network. The 7705 SAR supports ATM, TDM, and Ethernet.

7705 SAR MWA support

A packet microwave card is required to support MWA. The first four ports of the card are microwave aware. An MW link must be configured to enable MWA. MW link support includes 1+0 and 1+1 HSB protection. When configuring 1+1 HSB, each of the two radios is assigned a role of main radio or spare radio. By default, the main radio assumes the active status and the spare radio assumes the standby status. For 1+0 protection, MPT-HC, MPT-HCv2 and MPT-MC are supported. For 1+1 HSB protection, MPT-HC and MPT-HCv2 are supported.

1+1 HSB protection is displayed in the 5620 SAM physical topology map. The protection state is shown on the links, and 1+1 links are grouped in a common link group. The expansion of radio links on the physical map displays eight links. See section 6.2 for more information about the 5620 SAM physical topology map.



Note 1 — If the 9500 MPRe (version 4.2, standalone) is discovered before the 7705 SAR (single NE with 1+0 protection), the radio link is not shown on the topology map. Only after discovering the 7705 SAR will the radio link be shown on the topology map between the 7705 SAR and the 9500 MPRe.

Note 2 — 1+1 HSB protection is only supported between two 7705 SAR NEs.

The following protection types are supported:

- Radio Protection Switching (RPS)
  RPS is always supported in 1+1 radio configurations (HSB). RPS is implemented directly on a pair of MPTs.
- Transmission Protection Switching (TPS)
  TPS is always supported in 1+1 HSB radio configurations.
- Equipment Protection Switching (EPS)
  EPS protects the MPT and cables connecting the MPT to the IDU. RPS protection always assumes the MPT EPS.

See Procedure 15-11 for more information about configuring an MW link. See Procedure 15-12 for more information about configuring an MW link member.

7705 SAR NEtO support

The 5620 SAM supports an integrated MCT from the port or NE level on the 7705 SAR-8 and 7705 SAR-18. The MCT is distributed with a NEtO client in the 5620 SAM. The configuration of radio parameters is through the MCT. See Procedure 13-24 for more information about starting the MCT from the NE level.

7705 SAR auxiliary alarm daughter cards

The 7705 SAR supports an auxiliary alarm daughter card. This is a unique card that interfaces with real-time systems. The following inputs and outputs are available:

- 24 digital inputs that can connect to dry contacts of security sensors, HVAC systems, and telecom systems
- Two analog inputs for monitoring battery voltage; each supports a range of 0 to 75V and has configurable thresholds for alarms and events on each port
- Eight dry-contact relay outputs that interface to external audible, visual, or telecom equipment using NO or NC contact pins

The inputs and outputs are listed on the Ports tab of the daughter card slot properties form, in the same manner as ports on a data-plane daughter card. Each input or output has configurable parameters. The name specified for each input or output must be unique within the device.

7705 SAR 6-port E&M daughter cards

The 7705 SAR supports a six-port E&M daughter card. The configuration of ports and channels on this daughter card is similar to the 16-port DS1/E1 ASAP daughter card. You create a channel under each port, and a channel group under each channel.

The following configuration restrictions and limitations apply to ports and channels on the six port E&M daughter card:

- A port can have only one channel.
- A channel can have only one channel group.
- A channel group must be in Access mode and use CEM encapsulation.
- A channel group MTU is not configurable.

Only CESoPSN Cpipe SAPs can be created on the daughter card.

7705 SAR 12-port SDI card

The 7705 SAR-8 and 7705 SAR-18 support a 12-port Serial Data Interface card. The SDI card includes four connectors, each of which supports three ports. Each port in a three-port connector must be configured to work on the same interface type. The ports operate in access mode and can be configured to work with the following interfaces:

- RS232
- V.35
- X.21

RS232 interfaces support CEM encapsulation.

V.35 and X.21 interfaces support FR, CEM, HDLC, cHDLC, and IPCP encapsulation.

7705 SAR Power Injector card

The 7705 SAR-8 and 7705 SAR-18 support a Power Injector card to deliver power and data to an MPT radio. Up to four Power Injector cards can be installed on the 7705 SAR-8, and up to eight Power Injector cards can be installed on the 7705 SAR-18.

7705 SAR Optical Add/Drop Mux cards

The 7705 SAR-8 and 7705 SAR-18 support an Optical Add/Drop Mux (OADM) card in 1, 2, 4, and 8-colour variants. These cards increase bandwidth in a fiber network.

7705 SAR CSMv2 card

The 7705 SAR-8 supports a CSMv2 card. All of the 7705 SAR adapter cards are supported with the CSMv2. The 16p ASAPv1 does not support IP interfaces with the CSMv2. The CSMv2 card is similar in function to the CSMv1 card, however, the CSMv2 supports more deep channelized MDAs.



Note — A router cannot have a mix of CSMv1 and CSMv2 cards. To convert a router with CSMv1 hardware to CSMv2 hardware, the appropriate configuration files must be transferred to the new CSMv2.

7705 SAR 2 × 10-Gig Bridged Ethernet XFP + 1 × 2.5G Virtual Ethernet card

The 2 × 10-Gig Bridged Ethernet XFP + 1 × 2.5G Virtual Ethernet card connects to and from access rings carrying a high concentration of traffic. The 7705 SAR-8 supports up to 6 cards and the 7705 SAR-18 supports up to 12 cards. A single card can be installed on the 7705 SAR-8 and 7705 SAR-18.

The 2 × 10-Gig Bridged Ethernet XFP + 1 × 2.5G Virtual Ethernet card is also supported on the 7705 SAR-M ASAP and 7705 SAR-M with fan variants.

A number of 7705 SAR nodes in a ring typically aggregate traffic from customer sites, map the traffic to a service, and connect to an SR node. The SR node acts as a gateway point out of the ring. A 10GigE ring allows higher bandwidth services and aggregation on a per 7705 SAR basis.

In a deployment of a 2 × 10-Gig Bridged Ethernet XFP + 1 × 2.5G Virtual Ethernet card, each 7705 SAR node in the ring is connected to the east and west side of the rings over two different 10GigE ports. If 10GigE is the main uplink, two cards per 7705 SAR-8 are required for redundancy. With two cards per 7705 SAR-8 node, east and west links of the ring can be terminated on two different cards, reducing the impact of potential hardware failure. At initialization, the MAC address of the virtual port is programmed automatically. The card can operate in either LAN or WAN mode.

7705 SAR 6-port FXS Adapter card

The 7705 SAR-8 and 7705 SAR-18 support a 6-port FXS Adapter card that transports a large number of voice circuits from one 7705 SAR location to another 7705 SAR location, connected to a PBX. The card can also be configured for a PLAR application, which is typically used outside of a PBX network.

For a PBX application, the signal is terminated on an FXO interface at a 7705 SAR hub location that is connected to a PBX. The FXO interface can be either on an 8-port FXO Adapter card or 8-port Voice & Tele-protection card that is installed in a 7705 SAR-8 or 7705 SAR-18 chassis at the 7705 SAR-8 hub location. For a PLAR application, the signal is terminated on an FXS interface on either another 6-port FXS Adapter card or an 8-port Voice & Tele-protection card that is installed in a 7705 SAR-8 or 7705 SAR-18 chassis.

The 6-port FXS Adapter card has six FXS ports. Each port provides a short-reach, on-premises analog interface to an analog telephone set.

For standard TDM, the network interface can be a T1/E1 or OC3/STM1 channelized interface. For MPLS, an Ethernet, T1/E1, OC3/STM1 channelized MLPPP, or OC3/STM1 clear channel interface can be used.

The 6-port FXS Adapter card can be configured in access mode only.

7705 SAR 8-port FXO Adapter card

The 7705 SAR-8 and 7705 SAR-18 support an 8-port FXO Adapter card providing multiple FXO analog interfaces for connection to a PBX. The FXO analog interfaces can be connected over the MPLS network via a TDM pseudo wire (Cpipe) to an FXS interface on an 8-port Voice and Teleprotection card. The remote end can also be an FXS interface in a TDM multiplexer connected to the 7705 SAR by a T1/E1 interface. Each FXO interface separates the analog signal into two streams, one stream for voice and another for control signaling.

7705 SAR 10-port 1GigE/1-port 10GigE X-Adapter card

There are two versions of the 10-port 1GigE/1-port 10GigE X-Adapter card. The CLI identifier for version 1 is x-10GigE and for version 2, the CLI identifier is x-10GigE-v2. Both versions are identical except that version 2 is equipped with a hardware-based encryption engine that supports features such as IPsec.

The 10-port 1GigE/1-port 10GigE X-Adapter card can be configured for ten 1-gigabit ports or one 10-gigabit port. When configured for a one 10-gigabit port, the card can operate in either LAN or WAN mode. The card is supported on the 7705 SAR-18.

7705 SAR 8-port GigE SFP card (-48/+24 VDC)

There are three versions of the 8-port Gigabit Ethernet Adapter card. Version 1 and 2 are identical except that version 2 has more memory to support larger tables, such as FIBs and ACLs. Version 2 supports the full IPv6 subnet range for IPv6 static routes and interface IP addresses. Version 3 is identical to version 2 except that it is equipped with a hardware-based encryption engine that supports features such as IPsec. All versions are supported on the 7705 SAR-8 and the 7705 SAR-18.

7705 SAR Packet Microwave card

The 7705 SAR-8 and 7705 SAR-18 support the Packet Microwave card, 4 × MWA Gig Ethernet (2 TX, 2 SFP) + 4 × Gig Ethernet SFP. The 7705 SAR-8 supports up to 6 of these cards and the 7705 SAR-18 supports up to 12 cards. The first four ports of the Packet Microwave card are microwave ports and can be linked to a 9500 MPRe device.

7705 SAR Voice & Tele-Protection MDA

The 7705 SAR-8 and 7705 SAR-18 support the Voice & Tele-Protection MDA. The 7705 SAR-8 supports up to 6 cards and the 7705 SAR-18 supports up to 12 cards. Ports 1 and 2 support C37.94 interfaces, ports 3 and 4 support G.703 Co-directional interfaces, ports 5 and 6 support FXO interfaces, and ports 7 and 8 support FXS interfaces.

7705 SAR-A

The 7705 SAR-A is equipped with integrated twelve-port Ethernet MDA daughter cards. Depending on the variant, the 7705 SAR-A can support the configuration of eight Gig Ethernet, four Fast Ethernet, and eight T1/E1 ports. The two 7705 SAR-A daughter card variants are:

- integrated 12-port Ethernet, 8-port T1/E1, -48 VDC MDA
- integrated 12-port Ethernet, -48 VDC MDA

7705 SAR-F

The 7705 SAR-F integrates eight-port Ethernet v3 and 16-port DS1/E1 v2 ASAP MDA functions in one chassis. When the 5620 SAM discovers a 7705 SAR-F, the integrated MDAs are automatically configured and displayed in the equipment tree.

7705 SAR-H

The 7705 SAR-H is a hardened router and is based on the 7705 SAR-8, 7705 SAR-18, 7705 SAR-F, and 7705 SAR-M functionality. The 7705 SAR-H variants are:

- 7705 SAR-H high voltage shelf (88-264V AC/DC)
- 7705 SAR-H low voltage shelf (–48/–60 and +24 VDC)

The 7705 SAR-H provides firewall functions and applies a firewall to a layer 3 network, management, or CPM interface. The 7705 SAR-H firewall is a stateful firewall that provides the highest level of security. Stateful operation is a key feature in preventing DoS attacks from reaching the TCP/IP stacks of applications. The 7705 SAR-H employs a zone-based virtual firewall design.

The 5620 SAM allows you to configure the MDA mode of some MDA types on the 7705 SAR-H. There are two MDAs:

- Compact MDA, which is integrated in Slot 1 and has 8 Ethernet ports. The ports are configurable in the network or access mode.
  - ports 1 and 2 are gigabit Ethernet ports
  - ports 3 and 4 are combo ports
  - ports 5,6,7,8 are PoE port types
- Combo MDAs, which are modular type and used in Slot 2 and Slot 3, are configurable
  - ports 1 and 2 are serial ports
  - ports 3 and 4 are TDM ports

The 7705 SAR-H supports power supply tray objects which are automatically provisioned.

7705 SAR-M

The 7705 SAR-M variants are equipped with an integrated 7-port Ethernet card. Depending on the variant, a 7705 SAR-M may have an integrated 16-port channelized DS1/E1 ASAP card or a module slot. The 7705 SAR-M variants are:

- fan-cooled chassis with integrated 7-port Ethernet card, integrated 16-port channelized DS1/E1 ASAP card, and module slot
- fan-cooled chassis with integrated 7-port Ethernet card and module slot
- passively cooled chassis with integrated 7-port Ethernet card and integrated 16-port channelized DS1/E1 ASAP card
- passively cooled chassis with integrated 7-port Ethernet card

The following module cards can be inserted in the module slot:

- GPON module
- DSL module
- DCM
- 1 Colour Optical Add/Drop Mux module (OADM)

The DSL module includes a port with eight XDSL lines. The DCM includes one port with four SHDSL lines and one port with two XDSL lines. Except for 802.1x, 802.1ab LLDP, line loopbacks, and LAGs, all services and limitations which apply to Ethernet ports also apply to DCM and DSL modules.

7705 SAR-W

The 7705 SAR-W is equipped with an integrated daughter card that supports five data plane Ethernet ports: three SFP cages and two RJ-45 ports. The Ethernet ports are classified as permanent connections with primary surge protection. Depending on the variant of the card, the two RJ-45 ports will or will not support PoE. When the card is required to support NLOS/LOS microwave radio powered by PoE, the card needs RJ-45 ports with PoE capability. When PoE is not required, a low-cost and low-powered non-PoE card variant is available.

8.10 Workflow to manage 7705 SAR devices

The following workflow describes the sequence of high-level tasks required to commission, configure, and manage 7705 SAR NEs and services. This workflow assumes that the physical devices have been installed. The management functions are supplemental to the general management functions described in section 8.2.

1. Determine configuration requirements for the installed device; see this chapter, the *5620 SAM Network Element Compatibility Guide*, and the *5620 SAM Parameter Guide* for device specific information.
2. Commission the device for 5620 SAM management; see chapter 9 for more information. Configure polling policies as described in Procedure 9-4.
3. Perform 5620 SAM discovery of the commissioned network devices, and optionally configure SSH2 security for CLI sessions; see chapter 10 for more information.
4. As required, manage and configure equipment; see chapter 12 for more information about equipment management and configuration. Additionally, configure the following:
   - **a** TWAMP server as described in Procedure 13-11
   - **b** ICMP extensions as described in Procedure 13-21
   - **c** QoS ingress aggregate rates on the 7705 SAR-M as described in Procedure 13-23
   - **d** Launch an MCT from a 9500 MPR NE connected to a 7705 SAR as described in Procedure 13-24
   - **e** Timing synchronization as described in Procedure 15-7
   - **f** IEEE 1588 PTP clock as described in Procedures 15-8 and 15-9
   - **g** NTP as described in Procedure 15-10
   - **h** Microwave links and mw-link members as described in Procedures 15-11 and 15-12
   - **i** auxiliary alarm definitions as described in Procedure 15-13

j PoE ports as described in Procedures 16-19 and 16-20

k channelized TDM ports as described in Procedure 16-21

5 Create security policies and management access filters for NEs, and create NE user accounts that provide secure NE access using RADIUS or TACACS+ authentication. See "NE user and device security" in the *5620 SAM System Administrator Guide* for more information.

6 If required, perform NE maintenance functions such as backing up and restoring device configurations, upgrading device software, and monitoring deployment of configuration changes to devices. See "NE maintenance" in the *5620 SAM System Administrator Guide* for more information.

7 Create equipment inventories of managed devices; see chapter 17 for more information.

8 As required, perform additional device management functions such as the following:

a TCP enhanced authentication between NEs. See "TCP enhanced authentication" in the *5620 SAM System Administrator Guide* for more information

b threshold-crossing alarms; see chapter 19 for more information

c bulk configuration changes; see chapter 20 for more information

d automatic provisioning; see chapter 21 for more information

9 Configure NE routing and forwarding; see chapter 22 for general routing and forwarding information. As required, configure specific routing and forwarding functions such as the following:

a NE protocols; see chapter 23 for more information

b MPLS and LSPs; see chapter 25 for more information

c service tunnels to carry service traffic; see chapter 27 for more information

d Lawful Intercept; see chapter 28 for more information

e IPsec; see chapter 29 for more information

f 5620 SAM alarm policies; see chapter 31 for more information

g OAM diagnostic tests; see chapter 32 for more information

10 As required, configure redundancy in the managed network using functions such as the following:

a VRRP; see chapter 33 for more information

b APS; see chapter 34 for more information

c MC LAG groups; see chapter 39 for more information

11 Create 5620 SAM policies that define the conditions for 5620 SAM management functions; see chapter 42 for general information about 5620 SAM policy management. As required, configure specific policy types such as the following:

a QoS policies; see chapter 43 for more information. Additionally, configure a fabric profile as described in Procedure 43-26.

b filter policies; see chapter 44

c multicast policies; see chapter 45 for more information

d VRRP policies; see chapter 47 for more information

e auto tunnels policies; see chapter 48 for more information

f 802.1x policies; see chapter 50 for more information

g PBB MRP policies; see chapter 51 for more information

h connection profile policies; see chapter 53 for more information

i service PW template policies; see chapter 73 for more information

j residential subscriber policies; see chapter 54 for more information

k constraint policies; see chapter 56 for more information

l NAT policies; see chapter 57 for more information

m format and range policies; see chapter 58 for more information

n firewall policies; see chapter 60 for more information

12 Configure services and related functions; see chapters 61 and 62 for general service information. As required, configure specific services and related functions such as the following:

a virtual ports; see chapter 63 for more information

b customers; see chapter 64 for more information

c residential subscribers of customer services; see chapter 65 for more information

d VLL Apipe, Cpipe, Epipe, Fpipe, Ipipe, and Hpipe services to provide point-to-point connectivity between customer access ports; see chapter 67 for more information

e VPLS to provide virtual LAN connectivity that connects multiple customer sites in a bridged domain; see chapter 68 for more information

f mirror services for troubleshooting customer traffic issues or for use with Lawful Intercept; see chapter 69 for more information

g IES to provide an IP interface between customer traffic and the Internet; see chapter 70 for more information

h composite services to connect various types of services; see chapter 74 for more information

i 5620 SAM schedules and scheduled tasks to automate 5620 SAM service management functions such as running OAM diagnostics; see chapter 7 for more information

j OAM diagnostic tests into suites of manual and automatically-generated tests using the Service Test Manager; see chapter 77 for more information

k Ethernet Connectivity Fault Management; see chapter 78 for more information

l RCA audit; see chapter 80 for more information

8.11 7710 SR support

The Alcatel-Lucent 7710 SR is a modular, multi-service edge router that aggregates subscriber traffic over a variety of interfaces. It is based on the Alcatel-Lucent 7750 SR, and is typically deployed in distributed hub sites and enterprise customer offices to extend IP services to the network edge.

The 7710 SR chassis is optimized for the delivery of data, voice and video services, and supports up to 4 or up to 12 interfaces of various types and speeds.

8.12 Workflow to manage 7710 SR devices

The following workflow describes the sequence of high-level tasks required to commission, configure, and manage 7710 SR NEs and services. This workflow assumes that the physical devices have been installed. The management functions are supplemental to the general management functions described in section 8.2.

1 Determine configuration requirements for the installed device; see this chapter, the *5620 SAM Network Element Compatibility Guide*, and the *5620 SAM Parameter Guide* for device specific information.

2 Commission the device for 5620 SAM management; see chapter 9 for more information. Configure polling policies as described in Procedure 9-4.

3 Perform 5620 SAM discovery of the commissioned network devices, and optionally configure SSH2 security for CLI sessions; see chapter 10 for more information.

4 As required, manage and configure equipment; see chapter 12 for more information about equipment management and configuration. Additionally, configure channelized TDM ports as described in Procedure 16-22.

5 Create security policies and management access filters for NEs, and create NE user accounts that provide secure NE access using RADIUS or TACACS+ authentication. See “NE user and device security” in the *5620 SAM System Administrator Guide* for more information.

6 If required, perform NE maintenance functions such as backing up and restoring device configurations, upgrading device software, and monitoring deployment of configuration changes to devices. See “NE maintenance” in the *5620 SAM System Administrator Guide* for more information.

7 Create equipment inventories of managed devices; see chapter 17 for more information.

8 As required, perform additional device management functions such as the following:

- **a** TCP enhanced authentication between NEs. See “TCP enhanced authentication” in the *5620 SAM System Administrator Guide* for more information
- **b** threshold-crossing alarms; see chapter 19 for more information
- **c** bulk configuration changes; see chapter 20 for more information
- **d** automatic provisioning; see chapter 21 for more information

9 Configure NE routing and forwarding; see chapter 22 for general routing and forwarding information. As required, configure specific routing and forwarding functions such as the following:

- **a** NE protocols; see chapter 23 for more information
- **b** MPLS and LSPs; see chapter 25 for more information
- **c** service tunnels to carry service traffic; see chapter 27 for more information
- **d** Lawful Intercept; see chapter 28 for more information
- **e** IPsec; see chapter 29 for more information
- **f** 5620 SAM alarm policies; see chapter 31 for more information
- **g** OAM diagnostic tests; see chapter 32 for more information

10 As required, configure redundancy in the managed network using functions such as the following:

- **a** VRRP; see chapter 33 for more information
- **b** APS; see chapter 34 for more information
- **c** MC peer groups; see chapter 36 for more information
- **d** MC endpoint groups; see chapter 38 for more information
- **e** MC LAG groups; see chapter 39 for more information
- **f** MC synchronization groups; see chapter 40 for more information
- **g** MC ring groups; see chapter 41 for more information

11 Create 5620 SAM policies that define the conditions for 5620 SAM management functions; see chapter 42 for general information about 5620 SAM policy management. As required, configure specific policy types such as the following:

- **a** QoS policies; see chapter 43 for more information
- **b** filter policies; see chapter 44 for more information
- **c** multicast policies; see chapter 45 for more information

d time of day policies; see chapter 46 for more information

e VRRP policies; see chapter 47 for more information

f auto tunnels policies; see chapter 48 for more information

g RADIUS-based accounting policies; see chapter 49 for more information

h 802.1x policies; see chapter 50 for more information

i PBB MRP policies; see chapter 51 for more information

j connection profile policies; see chapter 53 for more information

k service PW template policies; see chapter 73 for more information

l residential subscriber policies; see chapter 54 for more information

m remote network monitoring policies; see chapter 55 for more information

n constraint policies; see chapter 56 for more information

o NAT policies; see chapter 57 for more information

p format and range policies; see chapter 58 for more information

12 Configure services and related functions; see chapters 61 and 62 for general service information. As required, configure specific services and related functions such as the following:

a virtual ports; see chapter 63 for more information

b customers; see chapter 64 for more information

c residential subscribers of customer services; see chapter 65 for more information

d VLL Apipe, Cpipe, Epipe, Fpipe, and Ipipe services to provide point-to-point connectivity between customer access ports; see chapter 67 for more information

e VPLS to provide virtual LAN connectivity that connects multiple customer sites in a bridged domain; see chapter 68 for more information

f mirror services for troubleshooting customer traffic issues or for use with Lawful Intercept; see chapter 69 for more information

g IES to provide an IP interface between customer traffic and the Internet; see chapter 70 for more information

h VPRN services to provides a virtual IP network that connects multiple customer sites; see chapter 71 for more information

i composite services to connect various types of services; see chapter 74 for more information

j 5620 SAM schedules and scheduled tasks to automate 5620 SAM service management functions such as running OAM diagnostics; see chapter 7 for more information

k OAM diagnostic tests into suites of manual and automatically-generated tests using the Service Test Manager; see chapter 77 for more information

l Ethernet Connectivity Fault Management; see chapter 78 for more information

m RCA audit; see chapter 80 for more information

8.13 7750 MG support

The 5620 SAM supports the discovery and management of the 7- or 12-slot Alcatel-Lucent 7750 MG. The 7750 MG can be configured with an SGW instance and a PGW instance in an LTE network.

The following documents describe 5620 SAM management and configuration of the 7750 MG:

- *5620 SAM LTE EPC User Guide*—Describes 7750 MG discovery, configuration, and management using the 5620 SAM
- *5620 SAM LTE Parameter Reference*—Describes 7750 MG device parameters as represented in the 5620 SAM schema, in addition to parameters on LTE and LTE service forms in the 5620 SAM GUI

8.14 7750 SR support

The Alcatel-Lucent 7750 SR is a multi-service edge router designed for service providers, cable MSO, and enterprise customers that deliver residential, business and mobile services through an IP/MPLS network.

The 5620 SAM supports the following 7750 SR chassis types:

- 7750 SR-1
- 7750 SR-7
- 7750 SR-12
- 7750 SR-c4
- 7750 SR-c12
- 7750 SR-12E

7750 SR-c4

The 7750 SR-c4, which supports up to 4 CMAs or 2 MDAs, has a forwarding capacity of 40 Gb/s, native uplink support, and a faster control plane processor than the 7750 SR. The ICM-2 is a preconfigured MDA that you cannot add or delete using the 5620 SAM.

The 7750 SR-c4 supports the following CMAs and MDAs:

- 7750 SR-c4 CFM-C4-XP
- 7750 SR-c4 IOM-C4-XP
- 5-port GIGE XP SFP CMA

- 1-port GIGE XP SFP CMA
- DC PEM

7750 SR-c12

The 7750 SR-c12, which supports up to 12 CMAs or 6 MDAs, has a forwarding capacity of 40 Gb/s, native uplink support, and a faster control plane processor than the 7750 SR.

7750 SR-12E

The 7750 SR-12E, which supports up to 12 CMAs or 6 MDAs, can deliver up to 200Gb/s per slot with full switch fabric redundancy. All features and applications supported by the 7750 SR-12 are supported on the 7750 SR-12E.

8.15 Workflow to manage 7750 SR devices

The following workflow describes the sequence of high-level tasks required to commission, configure, and manage 7750 SR NEs and services. This workflow assumes that the physical devices have been installed. The management functions are supplemental to the general management functions described in section 8.2.

1 Determine configuration requirements for the installed device; see this chapter, the *5620 SAM Network Element Compatibility Guide*, and the *5620 SAM Parameter Guide* for device specific information.

2 Commission the device for 5620 SAM management; see chapter 9 for more information. Configure polling policies as described in Procedure 9-4.

3 Perform 5620 SAM discovery of the commissioned network devices, and optionally configure SSH2 security for CLI sessions. See chapter 10 for more information.

4 As required, manage and configure equipment. See chapter 12 for more information. Additionally, configure the following:

   a mixed mode; see Procedure 15-6 for more information

   b IEEE 1588 PTP clock; see Procedures 15-8 and 15-9 for more information

5 Create security policies and management access filters for NEs, and create NE user accounts that provide secure NE access using RADIUS or TACACS+ authentication. See “NE user and device security” in the *5620 SAM System Administrator Guide* for more information.

6 If required, perform NE maintenance functions, such as the following:

   a backing up and restoring device configurations

   b upgrading device software

   c monitoring deployment of configuration changes to devices

   See “NE maintenance” in the *5620 SAM System Administrator Guide* for more information.

7 Create equipment inventories of managed devices. See chapter 17 for more information.

8 As required, perform additional device management functions, such as the following:

- **a** TCP enhanced authentication between NEs. See “TCP enhanced authentication” in the *5620 SAM System Administrator Guide* for more information
- **b** card migration; see chapter 18 for more information
- **c** threshold-crossing alarms; see chapter 19 for more information
- **d** bulk configuration changes; see chapter 20 for more information
- **e** automatic provisioning; see chapter 21 for more information

9 Configure NE routing and forwarding. See chapter 22 for general routing and forwarding information. As required, configure specific routing and forwarding functions, such as the following:

- **a** NE protocols; see chapter 23 for more information
- **b** MPLS and LSPs; see chapter 25 for more information
- **c** service tunnels to carry service traffic; see chapter 27 for more information
- **d** Lawful Intercept; see chapter 28 for more information
- **e** IPsec; see chapter 29 for more information
- **f** ISA-Video; see chapter 30 for more information
- **g** 5620 SAM alarm policies; see chapter 31 for more information
- **h** OAM diagnostic tests; see chapter 32 for more information

10 As required, configure redundancy in the managed network using functions such as the following:

- **a** VRRP; see chapter 33 for more information
- **b** APS; see chapter 34 for more information
- **c** MC peer groups; see chapter 36 for more information
- **d** MC endpoint groups; see chapter 38 for more information
- **e** MC LAG groups; see chapter 39 for more information
- **f** MC synchronization groups; see chapter 40 for more information
- **g** MC ring groups; see chapter 41 for more information

11 Create 5620 SAM policies that define the conditions for 5620 SAM management functions. See chapter 42 for general information about 5620 SAM policy management. As required, configure specific policy types, such as the following:

- **a** QoS policies; see chapter 43 for more information
- **b** filter policies; see chapter 44 for more information
- **c** multicast policies; see chapter 45 for more information
- **d** time of day policies; see chapter 46 for more information
- **e** VRRP policies; see chapter 47 for more information
- **f** auto tunnels policies; see chapter 48 for more information
- **g** RADIUS-based accounting policies; see chapter 49 for more information
- **h** 802.1x policies; see chapter 50 for more information
- **i** PBB MRP policies; see chapter 51 for more information
- **j** connection profile policies; see chapter 53 for more information
- **k** service PW template policies; see chapter 73 for more information
- **l** residential subscriber policies; see chapter 54 for more information
- **m** remote network monitoring policies; see chapter 55 for more information
- **n** constraint policies; see chapter 56 for more information
- **o** NAT policies; see chapter 57 for more information
- **p** format and range policies; see chapter 58 for more information

12 Configure services and related functions. See chapters 61 and 62 for general service information. As required, configure specific services and related functions, such as the following:

- **a** virtual ports; see chapter 63 for more information
- **b** customers; see chapter 64 for more information
- **c** residential subscribers of customer services; see chapter 65 for more information
- **d** VLL Apipe, Cpipe, Epipe, Fpipe, and Ipipe services to provide point-to-point connectivity between customer access ports; see chapter 67 for more information
- **e** VPLS to provide virtual LAN connectivity that connects multiple customer sites in a bridged domain; see chapter 68 for more information
- **f** mirror services for troubleshooting customer traffic issues or for use with Lawful Intercept; see chapter 69 for more information
- **g** IES to provide an IP interface between customer traffic and the Internet; see chapter 70 for more information

h VPRN services to provides a virtual IP network that connects multiple customer sites; see chapter 71 for more information

i composite services to connect various types of services; see chapter 74 for more information

j Application Assurance to provide deep-packet inspection and application-based subscriber traffic management; see chapter 76 for more information

k 5620 SAM schedules and scheduled tasks to automate 5620 SAM service management functions, such as running OAM diagnostics; see chapter 7 for more information

l OAM diagnostic tests into suites of manual and automatically-generated tests using the Service Test Manager; see chapter 77 for more information

m Ethernet Connectivity Fault Management; see chapter 78 for more information

n RCA audit; see chapter 80 for more information

8.16 7950 XRS support

The Alcatel-Lucent 7950 XRS is a large-scale routing system that is designed for core deployments. The 5620 SAM supports the management of the 7950 XRS including device discovery, equipment management, routing management, OAM, MPLS, QoS policies, and services.

Variants

The 5620 SAM supports the 7950 XRS-20 and the 7950 XRS-16c. The core feature set of the two variants is the same, but there are some physical differences that are described below.

7950 XRS-20

The 7950 XRS-20 has 20 XMA daughter card slots, which can be configured with XMA cards or compact XMA cards. The shelf includes two CCMs that support flash memory modules.

7950 XRS-16c

The 7950 XRS-16c is a lower capacity variant of the 7950 XRS. The shelf has 16 XMA daughter card slots, which can be configured only with compact XMA cards. Unlike the 7950 XRS-20, the 7950 XRS-16c shelf does not have a CCM. The flash memory modules are connected to the CPM.

Shelf components

You can monitor and manage the following 7950 XRS shelf components using the 5620 SAM navigation tree:

- CCMs
- XCM card slots; each slot has two XMA daughter card slots
- CPM card slots
- SFM card slots
- fan trays
- PEQ power supply trays

The number of the preceding components depends on the variant of the 7950 XRS.

The shelf components are N+1 redundant. The fan tray and power supply tray objects are automatically discovered and provisioned, and require no configuration using the 5620 SAM. See chapter 13 for more information about configuring shelf objects.

CCMs

The 7950 XRS-20 shelf includes two CCMs that support operator access to the routing system. You can view and monitor CCM and flash memory module properties from the CCM properties form. The CCMs are automatically detected and provisioned.

Each CCM includes three flash memory modules which can be viewed and monitored by the 5620 SAM. The “cf1” module is an internal flash module that is embedded in the system. The “cf2” and “cf3” modules are external compact flash slots.

XCM and XMA cards

The 7950 XRS-20 shelf includes ten XCM card slots that can be configured with XCM X20 cards. The 7950 XRS-16c shelf includes eight XCM card slots that can be configured with XCM X16 cards. Each XCM card can house up to two XMA cards for a total of twenty XMAs per 7950 XRS-20 shelf or sixteen XMAs per 7950 XRS-16c shelf. XMA card slots can also be configured with a compact XMA card, or C-XMA card. The 7950 XRS-16c can be configured only with C-XMA cards. The 5620 SAM supports the management of the following XMA/C-XMA types on the 7950 XRS:

- 20-port 10 GE SFP+ C-XMA
- 2-port 100 GE CFP C-XMA
- 6-port 40 GE QSFP C-XMA
- 40-port 10 GE SFP+ XMA
- 4-port 100 GE CXP XMA



Note — To configure the 40-port 10 GE SFP+ XMA or 4-port 100 GE CXP XMA cards on the 7950 XRS-20, you must configure SFM X20 B cards on the shelf. You cannot configure the XMA cards if the shelf is configured with SFM X20 cards.

CPM cards

The 7950 XRS shelf includes two redundant CPM card slots. Each slot is automatically provisioned with CPM X20 or CPM X16 cards, depending on the variant of the 7950 XRS.

On the 7950 XRS-20, each CPM card slot has an association with a CCM. If one of the components is removed, the appropriate status is applied to the corresponding CPM or CCM. In the 5620 SAM navigation tree, the CPM in Card Slot A is associated with CCM A. The CPM in Card Slot B is associated with CCM B.

On the 7950 XRS-16c, each CPM X16 card includes three flash memory modules, which can be viewed and monitored with the 5620 SAM. There is no associated CCM for the CPM X16.

SFM cards

The 7950 XRS shelf includes eight SFM card slots. SFM card slots on the 7950 XRS-20 can be configured with SFM X20 or SFM X20 B cards. SFM card slots on the 7950 XRS-16c can be configured with SFM X16 or SFM X16 B cards. You cannot configure a mix of SFM card types cards on one shelf. All configured slots must contain the same type of SFM card. Seven SFM cards must be operational to provide full capacity to the XCM cards, and one SFM card is redundant. At least one SFM card must be configured for the system to function.

8.17 Workflow to manage 7950 XRS devices

The following workflow describes the sequence of high-level tasks required to commission, configure, and manage 7950 XRS NEs and services. This workflow assumes that the physical devices have been installed. The management functions are supplemental to the general management functions described in section 8.2.

1. Determine configuration requirements for the installed device; see section 8.16, the *5620 SAM Network Element Compatibility Guide*, and the *5620 SAM Parameter Guide* for device specific information.
2. Commission the device for 5620 SAM management; see chapter 9 for more information.
3. Configure polling policies, as described in Procedure 9-4.
4. Perform 5620 SAM discovery of the commissioned network devices, and optionally configure SSH2 security for CLI sessions. See chapter 10 for more information.
5. If required, configure and manage equipment. See chapter 12 for more information.
6. Create security policies and management access filters for NEs, and create NE user accounts that provide secure NE access using RADIUS or TACACS+ authentication. See ”NE user and device security” in the *5620 SAM System Administrator Guide* for more information.

7 If required, perform any of the following NE maintenance functions:

- **a** Back up and restore the device configurations.
- **b** Upgrade the device software.
- **c** Monitor deployment of configuration changes to devices.

See “NE maintenance” in the *5620 SAM System Administrator Guide* for more information.

8 Create equipment inventories of the managed devices. See chapter 17 for more information.

9 If required, perform any of the following additional device management functions:

- **a** TCP enhanced authentication between NEs. See “TCP enhanced authentication” in the *5620 SAM System Administrator Guide* for more information
- **b** threshold-crossing alarms; see chapter 19 for more information
- **c** bulk configuration changes; see chapter 20 for more information
- **d** automatic provisioning; see chapter 21 for more information

10 If required, configure any of the following NE routing and forwarding functions. See chapter 22 for more information.

- **a** NE protocols; see chapter 23 for more information
- **b** MPLS and LSPs; see chapter 25 for more information
- **c** service tunnels; see chapter 27 for more information
- **d** lawful intercept; see chapter 28 for more information
- **e** alarm policies; see chapter 31 for more information
- **f** OAM diagnostic tests; see chapter 32 for more information

11 As required, configure redundancy in the managed network using functions such as the following:

- **a** VRRP; see chapter 33 for more information
- **b** MC peer groups; see chapter 36 for more information
- **c** MC endpoint groups; see chapter 38 for more information
- **d** MC LAG groups; see chapter 39 for more information
- **e** MC synchronization groups; see chapter 40 for more information
- **f** MC ring groups; see chapter 41 for more information

12 Create 5620 SAM policies that define the conditions for the 5620 SAM management functions. See chapter 42 for general information about 5620 SAM policy management. If required, configure any of the following policy types:

- **a** QoS policies; see chapter 43 for more information
- **b** filter policies; see chapter 44 for more information
- **c** multicast policies; see chapter 45 for more information
- **d** time of day policies; see chapter 46 for more information
- **e** auto tunnel policies; see chapter 48 for more information
- **f** 802.1x policies; see chapter 50 for more information
- **g** PBB MRP policies; see chapter 51 for more information
- **h** service PW template policies; see chapter 73 for more information
- **i** remote network monitoring policies; see chapter 55 for more information
- **j** constraint policies; see chapter 56 for more information
- **k** format and range policies; see chapter 58 for more information

13 If required, configure any of the following services and related functions. See chapters 61 and 62 for general service information.

- **a** customers; see chapter 64 for more information
- **b** VLL Epipe and Ipipe services to provide point-to-point connectivity between customer access ports; see chapter 67 for more information
- **c** VPLS to provide virtual LAN connectivity that connects multiple customer sites in a bridged domain; see chapter 68 for more information
- **d** mirror services for troubleshooting customer traffic issues or for use with lawful intercept; see chapter 69 for more information
- **e** IES to provide an IP interface between customer traffic and the Internet; see chapter 70 for more information
- **f** VPRN services to provides a virtual IP network that connects multiple customer sites; see chapter 71 for more information
- **g** composite services to connect various types of services; see chapter 74 for more information
- **h** schedules and scheduled tasks to automate 5620 SAM service management functions, such as running OAM diagnostics; see chapter 7 for more information
- **i** OAM diagnostic tests into suites of manual and automatically-generated tests using the Service Test Manager; see chapter 77 for more information
- **j** Ethernet CFM; see chapter 78 for more information
- **k** RCA audit; see chapter 80 for more information

8.18 9471 WMM support

The 9471 WMM provides MME and SGSN functions, terminating signaling traffic from UE, base stations, SGW, and other MME and SGSN to provide mobility functions and network access. The 9471 WMM equipment is represented in the 5620 SAM equipment navigation tree. Configurable parameters are displayed in the WMM instance. 5620 SAM support for the 9471 WMM includes the following:

- configuration management
- fault management
- PM statistics retrieval and storage
- pooling and bulk provisioning functions
- inventory management

The following documents describe 5620 SAM management and configuration of the 9471 WMM:

- *5620 SAM LTE EPC User Guide*—Describes 9471 WMM discovery, configuration, and management using the 5620 SAM
- *5620 SAM LTE Parameter Reference*—Describes 9471 WMM device parameters as represented in the 5620 SAM schema, in addition to parameters on LTE and LTE service forms in the 5620 SAM GUI

8.19 9500 MPR and 9500 MPRe support

The Alcatel-Lucent 9500 MPR is a microwave digital radio that supports PDH and Ethernet to migrate from TDM to IP. The 9500 MPR provides a generic, modular IP platform for multiple network applications, such as 2G, 3G, HSDPA, and WiMAX to accommodate broadband services.

The 9500 MPRe is the standalone, fully outdoor application of the MPT-MC ODU, with no shelf unit. The 9500 MPRe provides fixed or mobile Ethernet site backhauling and supports converged MPLS metro networks.

The following documents describe the 5620 SAM discovery, management, configuration, and administration of 9500 MPR/9500 MPRe devices.

- *5620 SAM User Guide*— Describes the tasks required to discover, configure, and manage 9500 MPR/9500 MPRe devices which do not differ from other device types managed by the 5620 SAM.
- *5620 SAM MPR User Guide*—Describes the unique tasks required to commission 9500 MPR/9500 MPRe devices, configure and manage the device objects, and configure and manage the policies and services associated with the device.
- *5620 SAM System Administrator Guide*—Describes the tasks required for security management, advanced configuration, and routine maintenance required for 9500 MPR/9500 MPRe devices and other device types.
- *5620 SAM Parameter Guide*—Provides a description of all GUI parameters that the 5620 SAM supports for 9500 MPR/9500 MPRe devices along with other device types.

8.20 eNodeB support

The eNodeB is an enhanced BTS system for UE access to the LTE RAN network and LTE services in the 700 MHz spectrum. The eNodeB is available as a compact or distributed system that consists of a BBU and a compact TRDU or distributed RRH component. Metro cell variants are also supported.

The following documents describe 5620 SAM management and configuration of the eNodeB:

- *5620 SAM LTE RAN User Guide*—Describes eNodeB discovery, configuration, and management using the 5620 SAM
- *5620 SAM LTE Parameter Reference*—Describes eNodeB device MIM parameters as represented in the 5620 SAM schema, in addition to parameters on LTE and LTE service forms in the 5620 SAM GUI

8.21 OmniSwitch support

The Alcatel-Lucent OmniSwitch family of devices is a group of Enterprise and Metro Ethernet LAN switches. The 5620 SAM supports the OmniSwitch chassis types listed in Table 8-3.

Table 8-3 5620 SAM OmniSwitch support

Family	Characteristics	AOS release supported	Chassis and cards support
OS 6250	Layer 2+ Fast Ethernet Stackable LAN family of switches which includes the OS 6250SME (small and medium enterprise) for the enterprise segment, and the OS 6250M, for the Metro access segment.	Release 6.6.4 or later	Non-PoE chassis • OS 6250-8M (Metro) • OS 6250-24M (Metro) • OS 6250-24MD (Metro) • OS 6250-24 (SME) PoE chassis • OS 6250-P24 (SME)
OS 6400	Stackable layer 2+ GigE LAN switch available in 24 or 48-port variants. Up to eight switches can be linked to form a stack.	Release 6.4.5 or later	Non-PoE chassis • OS 6400-24 • OS 6400-48 PoE chassis • OS 6400-P24 • OS 6400-P48 Fiber chassis • OS 6400-U24 • OS 6400-U24D

(1 of 4)

Family	Characteristics	AOS release supported	Chassis and cards support
OS 6450	Stackable GigE LAN switch available in 10-, 24-, or 48-ports variants, with optional upgrade paths for 10 GigE stacking, 10 GigE uplinks, and Ethernet (Metro) services.	Release 6.6.4 or later	Non-PoE chassis • OS 6450-10 • OS 6450-10L • OS 6450-24 • OS 6450-48 PoE chassis • OS 6450-P10 • OS 6450-P10L • OS 6450-P24 • OS 6450-P48 Fiber chassis • OS 6450-U24 Expansion port models • OS 6450-XNI-U2 • OS 6450-GNI-U2 • OS 6450-GNI-C2 Light models • OS 6450-C24-L • OS 6450-P24-L • OS 6450-C48-L • OS 6450-P48-L
OS 6850	Stackable layer 2/3 GigE fixed configuration switch available in 24 or 48-port variants. Up to eight switches can be linked to form a stack.	—	Non-PoE chassis • OS 6850-24 • OS 6850-24X • OS 6850-48 • OS 6850-48X • OS 6850-U24X • OS 6850-24L • OS 6850-48L PoE chassis • OS 6850-P24 • OS 6850-P24X • OS 6850-P48 • OS 6850-P48X • OS 6850-P24L • OS 6850-P48L
OS 6850E	The OS 6850E is the next evolution of the OS 6850. In addition to supporting the features of the OS 6850, the areas of enhancements for OS 6850E include form factor, new transceiver support, and new stacking mode.	Release 6.4.5 or later	Non-PoE chassis • OS 6850E-24 • OS 6850E-24X • OS 6850E-48 • OS 6850E-48X • OS 6850E-U24X PoE chassis • OS 6850-P24 • OS 6850E-P24X • OS 6850E-P48 • OS 6850E-P48X

(2 of 4)

Family	Characteristics	AOS release supported	Chassis and cards support
OS 6855	Stackable layer 2/3 GigE switch specifically built for IP network deployments where environmental operating conditions are unusually demanding. The OS 6855 is available with up to 24 gigabit ports and four combo ports.	Stackability only on OS6855-U24X chassis, Release 6.4.5 or later	Fiber chassis • OS 6855-U10 • OS 6855-U24 • OS 6855-U24X (stackable) Copper with PoE chassis • OS 6855-14 • OS 6855-24
OS 6900	The OS 6900 is a family of standalone aggregation switches that consists of two models: the OS 6900-X20 (640 Gb/s) and the OS 6900-X40 (1.28 Tb/s). The OS 6900-X40 has 40 fixed SFP+ ports, and two expansion slots. The OS 6900-X20 has 20 fixed SFP+ ports, and one expansion slot. Both models provide 1+1 redundant hot-swappable power supplies and a field-replaceable fan tray. Each expansion slot is capable of supporting 120 Gb/s of bandwidth.	Release 7.3.1 or later	XNI cards (supported on both model types) • OS-XNI-U12: Supports 12 SFP+ ports • OS-XNI-U4: Supports 4 SFP+ ports
OS 9600 (1)	A five-slot chassis supporting one CMM and four network interface modules. It offers a wide range of GigE and 10GigE interfaces and power-over-Ethernet to support IP telephones, WLAN access points and video cameras. The OS 9600 supports a maximum of two load sharing power supplies.	—	CMM cards • OS9600-CMM • OS9700-CMM • OS9800-CMM Network interface cards • 2-port 10GigE XFP • 6-port 10GigE XFP • 20-port Fast Ethernet (10/100 – SW upgradable to 10/100/1000) RJ45 and 2-port GigE (100/1000) SFP • 24-port GigE SFP • 24-port GigE (10/100/1000) RJ45 • 24-port GigE (10/100/1000) RJ45 w/PoE • OS9-GNI-P24: 24-port (10/100/1000) TX (RJ-45) PoE support • 48-port GigE (10/100/1000) MRJ21
OS 9700 (1)	A high-density ten-slot chassis with two slots for control and eight slots for network interfaces supporting an aggregation of up to 192 GigE ports or 48 10GigE ports. Designed for smart continuous switching operation, the two center slots are dedicated to CMMs allowing redundant configurations. The OS 9700 supports a maximum of three power supplies.	—	
OS 9800 (1)	A high performance 18-slot switch supporting 16 slots for GigE and/or 10-GigE network interface modules. An additional two slots are reserved for primary and redundant CMMs. The OS 9800 supports a maximum of four power supplies.	—	

(3 of 4)

Family	Characteristics	AOS release supported	Chassis and cards support
OS 9700E [2]	The OS 9700E is a high performance switch offering eight slots for GigE and/or 10-GigE Network Interface (NI) modules. Additional two slots are reserved for primary and redundant Chassis Management Modules (CMMs).	Release 6.4.5 or later	Network interface cards • OS9-GNI-C24E: 24-port 10/100/1000 with RJ-45 support • OS9-GNI-U24E: 24-port 1000base-X with SFP/MiniGBIC support • OS9-GNI-P24E: 24-port (10/100/1000) T/TX (RJ-45) PoE+ support • OS9-XNI-U2E: 2-port unpopulated 10-GigE with XFP support • OS9-XNI-U12E: Deployment fails if MPLS license is installed. Does not support MPLS/VPLS operations.
OS 9800E [2]	The OS 9800E is a high performance switch offering 16 slots for GigE and/or 10-GigE Network Interface (NI) modules. An additional two slots are reserved for primary and redundant Chassis Management Modules (CMMs).		
OS 10K [3]	The OS 10K is a high-capacity, high-performance modular Ethernet LAN switch that provides 5.12 Tb/s of switching performance. The OS 10K has a 12 slot chassis configuration: 4 slots for CMM/fabric cards; and 8 slots for XNI or GNI cards that provide Ethernet, GigE, and 10-GigE capabilities.	Release 7.3.1 or later	CMM and CFM cards • OS10K-CMM • OS10K-CFM XNI cards • OS10K-XNI-U32E: 32 unpopulated 10G SFP+ transceiver connectors • OS10K-XNI-U32S: 32 unpopulated 10G SFP+ transceiver connectors • OS10K-XNI-U16E: 16 unpopulated 10G SFP+ transceiver connectors GNI cards • OS10K-GNI-U48E: 48 SFP transceiver connectors • OS10K-GNI-C48E: 48 auto-sensing ports, each port is configurable as 10BaseT, 100BaseTX, or 1000BaseT QNI cards • OS10K-QNI-U4: 40-Gig network interface with pluggable QSFP transceiver connectors • OS10K-QNI-U8: 40-Gig network interface with pluggable QSFP transceiver connectors

(4 of 4)

Notes

(1) The 5620 SAM also supports the OS 9000 series of LAN switches which includes the OS 9600, OS 9700, and OS 9800.

(2) The 5620 SAM also supports the OS 9000E series of LAN switches which includes the OS 9700E and OS 9800E.

(3) The behavior of the power supplies is controlled by power management. You will see a power failure alarm even though power supplies are connected to the OS 10K chassis and is not being used by the 10K node. The 10K power management puts power supply into an inactive (down) state, if it is not required.



Caution 1 — OmniSwitch devices do not support automatic synchronization with the 5620 SAM database when you use the CLI to make configuration changes. To ensure that you are viewing accurate OmniSwitch information in the 5620 SAM, you must resynchronize the NE by clicking on the appropriate Resync button.

Caution 2 — OmniSwitch NEs do not send trap notifications for all MIB changes on the NE. To ensure that you are viewing the current configuration information in the 5620 SAM, you must resynchronize of the NE by clicking on the appropriate Resync button.

OmniSwitch LAG objects

OmniSwitch NEs support static and dynamic LAGs. When you create a static LAG, you can add ports as LAG members. The ports that you select as members of a dynamic LAG are first placed into an Unassigned Dynamic LAG Members group. The OmniSwitch uses LACP to dynamically assign ports from an Unassigned Dynamic LAG Members group to the appropriate LAG. When a port is assigned to a dynamic LAG, the port is removed from the Unassigned Dynamic LAG Members group.

You can create VLANs, use 802.1Q framing, configure QoS conditions, and enable other networking functions on a LAG, which is treated the same as physical link.

OmniSwitch LAG support includes:

- up to 32 LAGs on an OS 6250, OS 6400, OS 6450, OS 6850, OS 6850E, or OS 6855 on a stack of OmniSwitch devices
- up to 128 LAGs on an:
  - OS 9600, OS 9700, and OS 9800
  - OS 9700E or OS 9800E
  - OS 6900, Release 7.2.1 or later
  - OS 10K
- two, four, or eight Ethernet links in a LAG
- access or network LAGs

Using WebView to manage an OmniSwitch

You can configure and manage an OmniSwitch using the WebView application, an Alcatel-Lucent web-based element management tool that runs on an OmniSwitch. WebView supports the following web browsers:

- Internet Explorer 6.0 or later for Windows
- Netscape 7.1 for Windows

- Netscape 7.0 for Solaris
- Mozilla Firefox 10.0 or later for RHEL



Note — The web browser must have cookies and Java enabled.

See the appropriate OmniSwitch *Switch Management Guide* for information about configuring and using WebView. See chapter 13 for information about opening WebView using the 5620 SAM GUI.

8.22 Workflow to manage OmniSwitch devices

The following workflow describes the sequence of high-level tasks that are required to commission, configure, and manage OmniSwitch NEs and services. The workflow assumes that the physical devices are installed. The management functions are supplemental to the general management functions described in section 8.2.

1. Determine the configuration requirements for installed devices. See this chapter, the *5620 SAM Network Element Compatibility Guide*, and the *5620 SAM Parameter Guide* for specific device information.
2. Commission the device for 5620 SAM management; see Procedure 9-2 and chapter 9.
3. Perform 5620 SAM discovery of the commissioned network devices, and optionally configure SSH2 security for CLI sessions; see chapter 10.
4. As required, manage and configure equipment. See chapter 12 for more information about equipment management and configuration. Additionally, configure:
   - **a** LLDP; see Procedure 13-12.
   - **b** Ethernet diagnostics; see Procedures 13-26, 13-27, and 13-28.
   - **c** LAGs; see Procedures 14-12 and 14-13.
   - **d** running configuration; see Procedure 15-16.
   - **e** health monitoring; see Procedure 15-17.
   - **f** stacks; see Procedure 15-30.
   - **g** CPU temperature threshold; see Procedure 15-31.
   - **h** Ethernet ports; see Procedure 16-23.
   - **i** PoE ports; see Procedure 16-24.
5. Create RADIUS, TACACS+, or LDAP security policies. See “NE user and device security” in the *5620 SAM System Administrator Guide* for more information.

6 If required, perform any of the NE maintenance functions, such as:

a back up and restore device configurations.

b certify and synchronize device configurations.

c perform on-demand software upgrades or ISSUs.

d perform a software licence upgrade to allow OS 6250SME and OS 6450 NEs to perform in the Ethernet (Metro) role and support the OmniSwitch Ethernet (Metro) features.

e view a NE file system using an FTP file browser.

f monitoring the deployment of configuration changes to devices.

See "NE maintenance" in the *5620 SAM System Administrator Guide* for more information.

7 Create equipment inventories of managed devices. See chapter 17.

8 As required, perform additional device management functions, such as the following:

a TCP enhanced authentication between NEs. See "TCP enhanced authentication" in the *5620 SAM System Administrator Guide* for more information.

b threshold-crossing alarms; see chapter 19.

c bulk configuration changes; see chapter 20.

d automatic provisioning; see chapter 21.

9 Configure NE routing and forwarding. See chapter 22 for general routing and forwarding information. Additionally, configure the following, as required:

a OmniSwitch routing instances or VRF instances; see Procedures 22-5 and 22-1.

b UDP relay and DHCP Snooping on OmniSwitch routing instances; see Procedure 22-6.

c OmniSwitch L3 interfaces; see Procedures 22-11 and 22-12.

d OmniSwitch static routes; see Procedure 22-14.

10 As required, configure additional specific routing and forwarding functions, such as the following:

a NE protocols; see chapter 23. Additionally, configure:

- RIP; see Procedure 23-8.
- OSPF; see Procedures 23-24 to 23-31.
- PIM; see Procedures 23-39 and 23-40.
- IGMP; see Procedure 23-47.
- bridging; see Procedures 23-63 and 23-64.

b MPLS and LSPs; see chapter 25.

c service tunnels to carry service traffic; see chapter 27. Additionally, configure Ethernet ring elements; see Procedure 27-7.

d Lawful Intercept; see chapter 28.

e IPsec; see chapter 29.

f 5620 SAM alarm policies; see chapter 31.

g OAM diagnostic tests; see chapter 32. Additionally, configure ping and traceroutes; see Procedures 32-38, 32-40, and 32-41.

11 As required, configure redundancy in the managed network using functions such as the following:

a VRRP; see chapter 33.

b APS; see chapter 34.

12 Create 5620 SAM policies that define the conditions for 5620 SAM management functions. See chapter 42 for general information about 5620 SAM policy management. As required, configure specific policy types such as the following:

a QoS policies, actions, and conditions; see Procedures 43-34, 43-35, and 43-36, and chapter 43.

b filter policies; see chapter 44.

c multicast policies; see chapter 45.

d VRRP policies; see chapter 47.

e auto tunnels policies; see chapter 48.

f 802.1x policies; see chapter 50.

g PBB MRP policies; see chapter 51.

h AOS Ethernet service policies; see chapter 52.

i connection profile policies; see chapter 53.

j service PW template policies; see chapter 73.

k residential subscriber policies; see chapter 54.

l constraint policies; see chapter 56.

m NAT policies; see chapter 57.

n format and range policies; see chapter 58.

13 Configure services and related functions. See chapters 61 and 62 for general service information. As required, configure specific services and related functions such as the following:

a virtual ports; see chapter 63.

b customers; see chapter 64.

c residential subscribers of customer services; see chapter 65.

d VLAN services; see Procedures 66-1, 66-2, 66-3, 66-8, and 66-9, and chapter 66.

e VLAN groups; see chapter 66.

f VLL Apipe, Cpipe, Epipe, Fpipe, and Ipipe services to provide point-to-point connectivity between customer access ports; see chapter 67.

g VPLS to provide virtual LAN connectivity that connects multiple customer sites in a bridged domain; see chapter 68.

h mirror services for troubleshooting customer traffic issues or for use with Lawful Intercept; see chapter 69.

i IES to provide an IP interface between customer traffic and the Internet; see chapter 70.

j composite services to connect various types of services; see chapter 74.

k 5620 SAM schedules and scheduled tasks to automate 5620 SAM service management functions such as running OAM diagnostics; see chapter 7.

l OAM diagnostic tests into suites of manual and automatically-generated tests using the Service Test Manager; see chapter 77.

m Ethernet Connectivity Fault Management; see Procedure 78-5 and chapter 78.

n RCA audit; see chapter 80.

8.23 GNE support

The 5620 SAM provides limited SNMP management support of GNEs. Typically GNEs are non-Alcatel-Lucent devices, but the Alcatel-Lucent 9400 AWY and 9500 MSS-1c are treated as GNEs by the 5620 SAM. 5620 SAM support for GNEs is limited to the following:

- discovery and display on topology maps (GNE only, not its interfaces)
- inclusion in the navigation tree (GNE only, not its interfaces)
- physical link creation and representation
- generic trap translation into 5620 SAM alarms
- status polling using enterprise MIB object interface alarms

- telnet, SSH, and web sessions can be launched
- provisioning using CLI scripts
- inclusion in a service instance created with scripts from, and managed by, the 5620 SAM.



Note 1 — By default, only the 5620 SAM admin user, or an operator with an assigned admin scope of command role, can manage GNE profiles and alarm catalogues. A non-admin user requires the genericne scope of command role to manage GNE profiles.

Note 2 — To create, modify, or delete a GNE alarm catalogue or mapping, you require a trapmapper scope of command role with write, update, and execute permissions.

Note 3 — From a 5620 SAM discovery and management perspective, the Alcatel-Lucent 9400 AWY and 9500 MSS-1c are considered to be GNEs. See Procedure 9-9 for information about how to discover and manage these device types.

GNE device discovery and polling in the 5620 SAM are configured using the same methods that are used for Alcatel-Lucent devices, but the 5620 SAM uses preconfigured scripts to manage and unmanage a GNE. See the chapter 10 for information about device discovery. See chapter 20 for information about creating CLI scripts using the 5620 SAM Scripts tool.

Statistics support

The 5620 SAM supports the collection of a limited set of statistics counters from standard system, interface, and routing MIBs on GNEs. These statistics are processed and presented in the same manner as statistics from other devices. You can view GNE statistics on the Statistics tab of a GNE interface properties form, retrieve them using the OSSI, and display them graphically using the 5620 SAM Statistics Plotter.



Note 1 — To collect or view GNE statistics from routing MIBs, you require a valid 5650 CPAM license that has a third-party router quantity greater than zero.

Note 2 — If persistent SNMP indexes are not enabled on a GNE, one or more GNE interface indexes may change after a GNE reboots. This can cause a mismatch between the statistics records collected before the reboot and the current interface indexes. The 5620 SAM takes no action to identify or correct such a mismatch.

See “Statistics collection configuration” in the *5620 SAM Statistics Management Guide* for general information about configuring and collecting statistics.

Alarm support

By default, the 5620 SAM supports a limited number of standard system and interface SNMP traps for GNEs. The 5620 SAM monitors SNMP reachability and interface status, and raises a standard alarm for each the following events:

- coldStart—The GNE restarts.
- linkDown—An interface goes out of service.
- linkUp—An interface returns to service.



Note — When the 5620 SAM drops or fails to receive an SNMP trap from a GNE, the trap is lost. The 5620 SAM is unable to request that a GNE resend an SNMP trap.

You can configure the 5620 SAM to raise user-defined alarms in response to specific GNE traps using alarm catalogues. See section 9.2 for information about configuring user-defined alarms for GNEs.

GNE alarm catalogues

An alarm catalogue is a set of trap-to-alarm mappings that can be associated with a GNE profile. A GNE profile can have at most one alarm catalogue, but each catalogue can contain up to 150 alarm mappings. When a mapping is administratively disabled, the 5620 SAM raises no alarm in response to an associated trap from a GNE.

An alarm mapping can be static, which means that it maps to a specific alarm, or the mapping can use one or more transform functions that extend the mapping customization. A transform function defines conditions that enable the dynamic mapping of a trap to an alarm that is created using varbind values in an SNMP trap PDU. For example, you can use a transform function to assign a specific alarm name, severity, or probable cause to an alarm based on varbind values.

You can use a 5620 SAM GUI or OSS client to configure GNE alarm catalogues and alarm mappings. The GUI supports the following methods:

- configuration forms—for object creation, modification, viewing, and deletion

  See chapter 9 for information about managing GNE alarm catalogues using configuration forms.
- XML API script—for object creation and modification only

  A script template for alarm catalogue configuration is available at the following location:

  install_dir/nms/sample/xmlapi/AlarmCatalogue-Template.txt

  where *install_dir* is the 5620 SAM main server installation directory, typically /opt/5620sam/server

See "Creating and executing scripts" in the *5620 SAM Scripts and Templates Developer Guide* for information about using the Scripts tool.

An OSS client can also retrieve a catalogue or a subset of the alarm mappings in a catalogue using the standard methods.

When the 5620 SAM receives a GNE trap that is not one of the supported standard traps or a mapped trap in an alarm catalogue, the 5620 SAM drops the trap. When the 5620 SAM receives a high trap volume and must discard traps that it cannot process, it does not distinguish between standard and user-defined traps. To conserve system resources, Alcatel-Lucent recommends that you configure a GNE to send only the required traps to the 5620 SAM.

Traps that map to user-defined alarms require extra processing by the 5620 SAM and are managed in a separate, resource-limited queue. When this queue fills, the 5620 SAM discards some of the traps and raises an alarm. You can monitor the queue length using the 5620 SAM Resource Manager.

GNE trap sequencing and throttling support are configurable in a GNE profile. After the 5620 SAM finishes throttling traps from a GNE or encounters a trap sequence error, it resynchronizes the discovered device MIBs.

8.24 Workflow to manage GNEs

The following workflow describes the sequence of high-level tasks that are required to commission, configure, and manage GNEs and services. The workflow assumes that the physical devices are installed. The management functions are supplemental to the general management functions described in section 8.2.

1 Non-admin users require an assigned GNE scope of command role to manage GNEs. See section 9.1 and the *5620 SAM System Administrator Guide* for more information.

2 Perform the commissioning preconfiguration on the GNE before the 5620 SAM can manage it by creating a GNE profile. See section 9.1 for more information.

3 As part of a GNE profile creation, you can optionally map SNMP traps from GNEs to user-defined 5620 SAM alarms in an alarm catalogue. See section 9.1 for more information.

4 Create a mediation policy with the same SNMP settings that were specified during the GNE preconfiguration; see chapter 10.

5 Perform 5620 SAM discovery of the commissioned GNEs, and optionally configure SSH2 security for CLI sessions; see chapter 10.

6 As required, manage and configure equipment. See chapter 12 for more information about equipment management and configuration.

7 As required, configure additional specific routing and forwarding functions, such as the following:

   a NE protocols; see chapter 23. Additionally, configure:

      - RIP; see Procedure 23-8.
      - OSPF; see Procedures 23-24 to 23-31.
      - PIM; see Procedures 23-39 and 23-40.
      - IGMP; see Procedure 23-47.
      - bridging; see Procedures 23-63 and 23-64.

   b MPLS and LSPs; see chapter 25.

c service tunnels to carry service traffic; see chapter 27. Additionally, configure Ethernet ring elements; see Procedure 27-7.

d Lawful Intercept; see chapter 28.

e IPsec; see chapter 29.

f 5620 SAM alarm policies; see chapter 31.

g OAM diagnostic tests; see chapter 32. Additionally, configure ping and traceroutes; see Procedures 32-38, 32-40, and 32-41.

8 Create 5620 SAM policies that define the conditions for 5620 SAM management functions. See chapter 42 for general information about 5620 SAM policy management. As required, configure specific policy types such as the following:

a QoS policies, actions, and conditions; see Procedures 43-34, 43-35, and 43-36, and chapter 43.

b filter policies; see chapter 44.

c multicast policies; see chapter 45.

d VRRP policies; see chapter 47.

e auto tunnels policies; see chapter 48.

f 802.1x policies; see chapter 50.

g PBB MRP policies; see chapter 51.

h AOS Ethernet service policies; see chapter 52.

i connection profile policies; see chapter 53.

j service PW template policies; see chapter 73.

k residential subscriber policies; see chapter 54.

l constraint policies; see chapter 56.

m NAT policies; see chapter 57.

n format and range policies; see chapter 58.

9 Configure services and related functions. See chapters 61 and 62 for general service information. As required, configure specific services and related functions such as the following:

a virtual ports; see chapter 63.

b customers; see chapter 64.

c residential subscribers of customer services; see chapter 65.

d VLAN services; see Procedures 66-1, 66-2, 66-3, 66-8, and 66-9, and chapter 66.

e VLAN groups; see chapter 66.

f VLL Apipe, Cpipe, Epipe, Fpipe, and Ipipe services to provide point-to-point connectivity between customer access ports; see chapter 67.

g VPLS to provide virtual LAN connectivity that connects multiple customer sites in a bridged domain; see chapter 68.

h mirror services for troubleshooting customer traffic issues or for use with Lawful Intercept; see chapter 69.

i IES to provide an IP interface between customer traffic and the Internet; see chapter 70.

j composite services to connect various types of services; see chapter 74.

k 5620 SAM schedules and scheduled tasks to automate 5620 SAM service management functions such as running OAM diagnostics; see chapter 7.

l OAM diagnostic tests into suites of manual and automatically-generated tests using the Service Test Manager; see chapter 77.

m Ethernet Connectivity Fault Management; see Procedure 78-5 and chapter 78.

n RCA audit; see chapter 80.

9 — Device commissioning and management

9.1 Device commissioning overview *9-2*

9.2 GNE commissioning overview *9-6*

9.3 Workflow to commission Alcatel-Lucent devices *9-9*

9.4 Device commissioning procedures *9-10*

9.5 Workflow to commission GNEs *9-24*

9.6 GNE commissioning procedures *9-25*

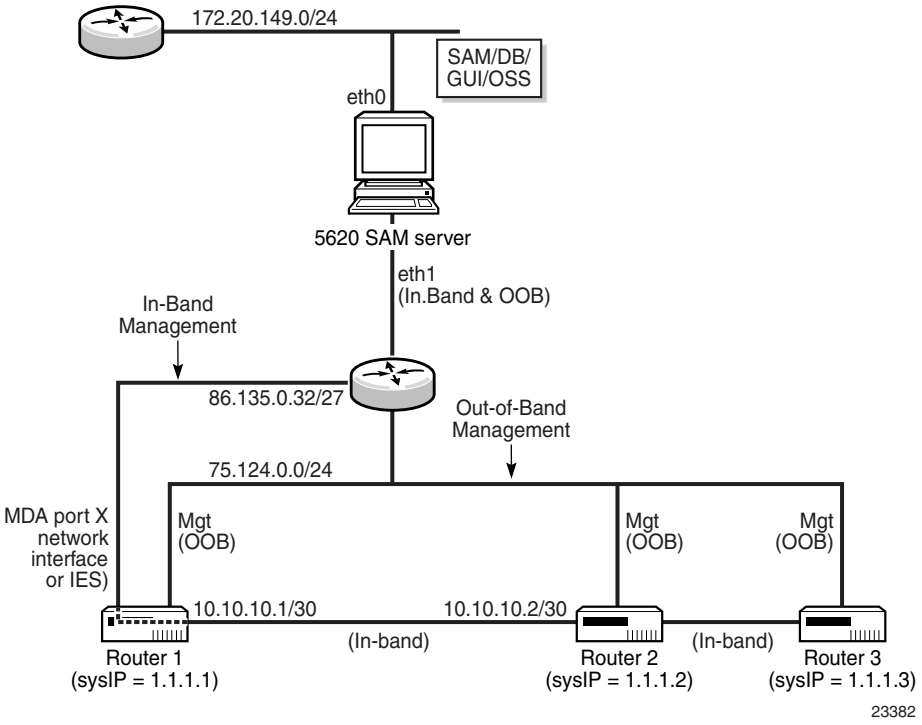
9.1 Device commissioning overview

An Alcatel-Lucent device or GNE requires preconfiguration before 5620 SAM management of the device is possible. When the preconfiguration is complete, the 5620 SAM can discover the device, as described in chapter 10. See section 9.3 for the device commissioning workflow.

In-band and out-of-band management

The 5620 SAM supports the in-band and out-of-band management of devices. Figure 9-1 shows an example of in-band and out-of-band management.

Figure 9-1 Example of in-band and out-of-band management



When you configure only in-band management, management traffic between the 5620 SAM and a device is transmitted through any port that is configured for network access, except the management port. For in-band management, the 5620 SAM sends management traffic to the device system IP address, or to an optionally specified L3 management interface.

When you configure only out-of-band management, management traffic between the 5620 SAM and a device is transmitted through the management port of the device. For out-of-band management, the 5620 SAM sends management traffic to the management IP address of the device.

When a device is configured for in-band and out-of-band management, one method provides management redundancy for the other. However, if the in-band and out-of-band IP addresses are the same, the 5620 SAM cannot determine which NE interface is active, and management redundancy is compromised. If the in-band and out-of-band IP addresses are the same on a newly discovered NE, the 5620 SAM raises an alarm.

Note 1 — The OmniSwitch does not support management redundancy.

Note 2 — The 5620 SAM uses one SNMP trap target for in-band and out-of-band management. The 5620 SAM SNMP IP address must be routable from each IP address when in-band and out-of-band management are used. See the device documentation for information about configuring an SNMP trap target.

The type of management is determined during device discovery. When the device is discovered using its management IP address, system IP address, or L3 interface IP address, the in-band and out-of-band addresses are synced in the 5620 SAM. This enables configuration of management redundancy, if both in-band and out-of band are available. In each case, a valid route to the device must exist. See chapter 10 for more information about the discovery process.

In Figure 9-1, an out-of-band management route allows a ping from the 5620 SAM to the management IP address of Router 1 (192.168.10.1/32). The in-band connection sends management packets to the system IP address on Router 2 (12.12.12.2/32) on MDA port X.

Caution — Do not use the 5620 SAM to modify the configuration of the in-band port. If the port is shut down, network visibility is lost.

Note — In Figure 9-1, the IP addresses for Router 1 and 2 each end with /mask. This value needs to changed for another value. Many values can be selected but the following values are most common:

- /31 for two hosts
- /30 for two hosts with network and broadcasts numbers
- /24 for 254 hosts

Some device types require configuration in addition to the SNMP configuration before they can be managed by the 5620 SAM. See the appropriate part of this section for device-specific management information.

7705 SAR management bandwidth

Some additional bandwidth management configuration is required with the 5620 SAM, if you want to transmit on in-band management on the 7705 SAR. Currently, if in-band and out-of-band management are both used, then the 7705 SAR will only transmit on the out-of-band management out-of-preference if that route exists.

You need to configure 5620 SAM so that each 7705 SAR with out-of-band management connectivity has the following parameter values:

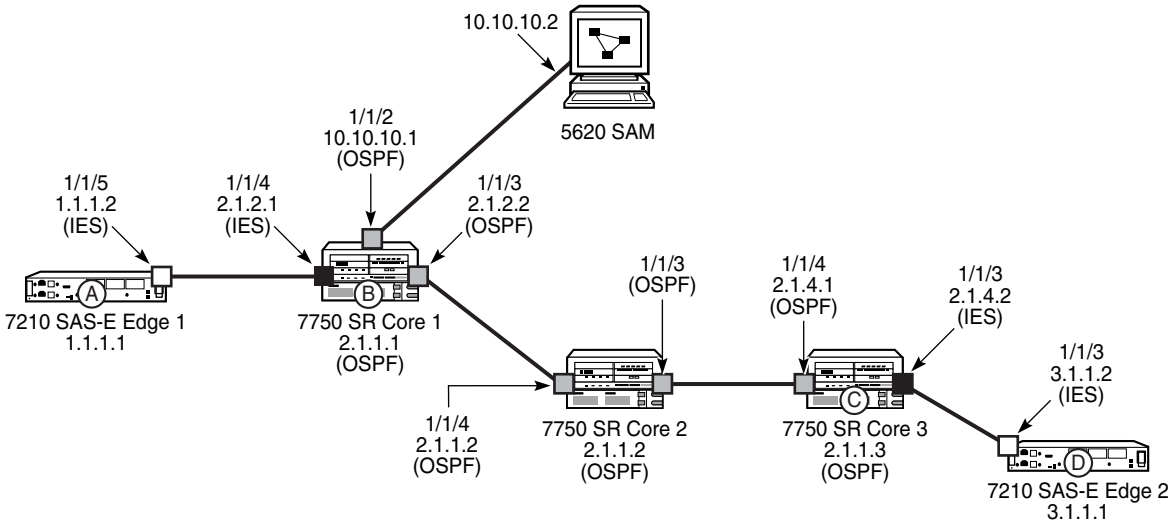
- Active Management IP - In Band
- Auto Revert to Preferred - True or False
- Management IP selection - in Band Preferred

See Procedure 9-4 for the steps on how to configure these values.

7210 SAS in-band and out-of-band management

The 7210 SAS supports in-band and out-of-band management. The 7210 SAS-D and 7210 SAS-E support static routes, but do not support an IGP or SDPs. The example network shown in Figure 9-2 and the associated configuration steps describe the configuration required to enable 7210 SAS-E in-band management using static routes that are distributed to an IGP, which, in the example, is OSPF.

Figure 9-2 Example 7210 SAS-E in-band management network



Ⓐ static-route 10.10.10.0/24 next-hop 2.1.2.1, static-route 2.1.1.0/24 next-hop 2.1.2.1

Ⓑ static-route 1.1.1.1/32 next-hop 1.1.1.2, Distribute the static routes to OSPF

Ⓒ static-route 3.1.1.1/32 next-hop 3.1.1.2, Distribute the static routes to OSPF

Ⓓ static-route 10.10.10.0/24 next-hop 2.1.4.2, static-route 2.1.1.0/24 next-hop 2.1.4.2

Legend:
- Access uplink port
- Access port
- Network port

20259

The following configuration steps are required to set up the example network:

1 Using the CLI, configure the SNMP security parameters on the devices that you need to discover. See Procedure 9-1 for more information.

2 Perform the following steps on Core 1.

- Configure an interface on port 1/1/2 that connects to the 5620 SAM server interface.
- Configure an interface on port 1/1/3, which is connected to Core 2.
- Create an L3 interface on port 1/1/4 by creating an IES.
- Create a static route to Edge 1.
- Create an ASBR OSPF (area 0.0.0.0) instance on the system and enable OSPF on the interfaces to Core 2 and the 5620 SAM server.
- Create a routing policy to distribute the static route to OSPF.

3 Perform the following steps on Core 2.

- Configure an L3 interface on port 1/1/4, which is connected to Core 1.
- Configure an L3 interface on port 1/1/3, which is connected to Core 3.
- Enable OSPF (area 0.0.0.0) on the system and the interfaces connected to Core 1 and Core 3.

4 Perform the following steps on Core 3.

- Create an L3 interface on port 1/1/4, which is connected to Core 2.
- Create an L3 interface on port 1/1/3, which is connected to Edge 2.
- Create a static route to Edge 2.
- Create an ASBR OSPF (area 0.0.0.0) instance on the system and enable OSPF on the interface to Core 2.
- Create a routing policy to distribute the static route to OSPF.

5 Perform the following steps on Edge 2.

- Create an IES L3 interface on port 1/1/3, which is an uplink port.
- Create static routes that direct traffic to the IES L3 interface.

6 Perform the following steps on Edge 1.

- Create an IES L3 interface on port 1/1/5, which is configured as an uplink port.
- Create static routes to direct traffic to the IES L3 interface.

7 Ensure that each 7210 SAS-E can ping the network interface IP address which is configured on the 5620 SAM main server.

8 Ensure that the 5620 SAM main server can ping the system IP address of each 7210 SAS-E.

9 Configure an in-band polling policy using the 5620 SAM. See Procedure 9-5 for more information.

Firewalls and management bandwidth

The ports between 5620 SAM components, and between the 5620 SAM system and the managed devices, must be open through firewalls to allow proper operation of the software. See the *5620 SAM Planning Guide* for more information about requirements for the following:

- firewalls and open ports
- communication bandwidth between 5620 SAM components
- communication bandwidth between the 5620 SAM and managed network

IPv6 device management

The 5620 SAM supports device management using IPv6 for devices with IPv6 capabilities. The management protocol is established when the device is discovered. When a device is configured with an IPv6 address on its management port and/or system interface and the discovery rule is configured to discover IPv6 addresses, the 5620 SAM discovers and manages the device using IPv6. To change a device management protocol between IPv4 and IPv6, you must unmanage the device, create a new discovery rule specifying the new management protocol, and then rediscover the device.



Note 1 — To manage 7750 SR, 7710 SR, 7450 ESS, or 7950 XRS devices using IPv6, the device must also be configured with an IPv4 address on the management port for out-of-band management, or an IPv4 address on the system interface for in-band management.

Note 2 — To manage the 7210 SAS-E, 7210 SAS-M, 7210 SAS-T, or 7210 SAS-X, Release 4.0 or later using IPv6 for out-of-band management, you must configure IPv6 on the management port and IPv4 on the system interface. Earlier releases of the 7210 SAS do not support IPv6 management.

The 7210 SAS-D, 7210 SAS-M, 7210 SAS-T, and 7210 SAS-X, Release 5.0 R1 or later, support in-band management using IPv6.

The 5620 SAM supports the configuration of IPv4 and IPv6 in-band and out-of-band management addresses on the same device.

Secure file transfers

The 5620 SAM supports secure and non-secure file transfers for backups, restores, software upgrades, and statistics collection. The device mediation policy determines whether FTP or SCP is used to perform file transfers to and from the managed devices. SCP requires SSH2. See chapter 10 for more information about configuring SSH2.

9.2 GNE commissioning overview

A GNE requires commissioning preconfiguration before the 5620 SAM can manage it. When the preconfiguration is complete, the 5620 SAM can discover the device, as described in chapter 10.

The 5620 SAM uses configurable profiles and CLI configuration scripts to discover and manage GNEs. You can use one GNE profile for multiple GNEs of the same type.

By default, only the 5620 SAM admin user, or a user with an assigned admin scope of command role, can manage GNE objects. To create and configure GNE objects, a non-admin user requires a scope of command role that has Create and Update/Execute permissions on packages and classes that include the following:

- genericne—to create GNE interfaces and configure profiles
- netw—to create discovery rules
- script—to manage scripts

- security.MediationPolicy and snmp.PollerManager—to create mediation policies
- trapmapper—to create alarm catalogs that map SNMP traps to 5620 SAM alarms

The 5620 SAM can discover a device as a GNE only when the following conditions are in place.

- The GNE preconfiguration is complete.
  - The System Object ID of the GNE is required for the GNE Profile, for example 1.3.6.1.4.1. When multiple GNE profiles contain possible matches for a system object ID, the profile that contains the system object ID with the longest or most specific match is chosen.
  - SNMP is configured and enabled on the device.
  - Telnet or SSH is enabled on the device.
- A 5620 SAM GNE profile for the device exists.
- A 5620 SAM mediation policy is configured with SNMP settings that match the device configuration.
- A discovery rule for the device exists.

See section 9.5 for the GNE commissioning workflow. See chapter 10 for information about mediation policies and device discovery.

Using alternate element managers

If an EMS client application for a GNE is installed on a 5620 SAM GUI client station, you can use a right-click GNE menu option in the network navigation tree to open the EMS client application. The OS-level command that opens the client must be specified in the associated GNE profile, or in the individual GNE configuration, to enable the function. A command in the configuration of a specific GNE overrides a command in the associated GNE profile.

If the command path is not included, the 5620 SAM attempts to locate the command using the paths listed in the PATH environment variable of the client station OS.

If the command that opens an EMS client accepts an NE IP address as an argument, you can specify the address using a keyword in the command entry. The 5620 SAM replaces the keyword with the target GNE IP address as it runs the command.

An alternate GNE manager is configurable using the GUI or OSS. See Procedure 9-7 for information about configuring an alternate EMS in a GNE profile. See Procedure 9-8 for information about specifying an alternate EMS in the GNE configuration.

GNE profiles

5620 SAM management of a device as a GNE requires a GNE profile, which defines how the 5620 SAM communicates with the device. A GNE profile includes the following elements:

- a unique GNE name
- the system object ID from the device MIB
- the GNE category
- the interface types that the GNE supports
- the interfaces that can be specified as the endpoints of 5620 SAM physical links

- an SNMP trap management configuration that associate trap configuration and deconfiguration scripts with the profile
- CLI profile information
- an optional alarm catalog that defines the alarms that the 5620 SAM raises in response to SNMP traps from the device

Configuring user-defined alarms for GNEs

You can map GNE SNMP traps to user-defined 5620 SAM alarms in an alarm catalog, and associate the catalog with a GNE profile. A GNE profile can have one alarm catalog that contains up to 150 trap-to-alarm mappings.

A mapping is one of the following types:

- static—A specific SNMP trap is associated with a specific alarm.
- dynamic—The mapping includes one or more transform functions that define alarm properties based on values in SNMP trap PDUs.

Each mapping in a catalog defines an alarm that the 5620 SAM raises or clears when it receives a specific SNMP trap. A mapping includes standard elements such as the trap OID, alarm type, probable cause, and severity, but can include the following optional elements:

- trap name
- self-clearing designation—specifies that the alarm clears when a specific clearing trap is received, and has the following requirements:
  - If the severity of the raising alarm is a static value, the clearing trap must have a static mapping in the same catalog as the raising trap, and can be linked to only one raising trap.
  - If the severity of the raising alarm is defined using a transform function, the transform function must include a raising value pair and a clearing value pair.
- FDN extension, which is an alarm-name extension that can include the following:
  - static text
  - scripting functions—expressions that specify the trap PDU values to include; these allow the same alarm type to be raised in response to different traps while uniquely identifying the trap origin in the alarm name.
- additional text—used to provide information of value related to the trap event, for example, troubleshooting actions; the additional text consists of the trap OID by default, but can include the following:
  - static text
  - scripting functions—expressions that specify the trap PDU values to include; these are used to generate a more precise description of the alarm condition
- System Address and/or Interface Index varbind positions for a GNE on which to raise an alarm



Note — The FDN extension of a GNE alarm is not appended to the Alarm Name field in the 5620 SAM GUI, but is included in the Additional Text field. To create a filter for GNE alarms that have FDN extensions, you must filter on the Additional Text field.

A change to an alarm catalog or to a mapping in a catalog takes effect immediately after you commit the change.

Transform functions

A transform function is an optional catalog component that associates one or more values in an SNMP trap PDU with an alarm property such as the alarm name, probable cause, or severity. For example, you can create a transform function that assigns an alarm severity of Critical when the value in a specific varbind is 1, Major when the value is 2, and Minor when the value is 3.

When an alarm mapping includes one or more transform functions, the 5620 SAM can raise multiple alarms in response to the same SNMP trap. A trap value and the associated alarm property value are specified as a value pair in a transform function. You can also specify a default alarm property value that the 5620 SAM assigns to an alarm when a received value is not defined in a value pair.

A transform function defines the input value type, such as integer, and the output alarm property type, such as severity. You can modify these parameters only when the transform function does not contain a value pair and is not used by a mapping.

A transform function returns an empty string when a received value is not defined in a value pair and no default alarm property value is assigned. When the transform function defines the alarm name, probable cause, or severity, the 5620 SAM logs an error in response and does not raise an alarm.

9.3 Workflow to commission Alcatel-Lucent devices

The following workflow describes the high-level tasks required to commission a device prior to discovery by the 5620 SAM.

1. Enable and configure SNMP on the device.
   - **a** See Procedure 9-1 for 5620 SAM natively-managed devices.
   - **b** See Procedure 9-2 for the OmniSwitch.
2. If required, configure the source of device SNMP traps; see Procedure 9-3.
3. If required, use a CLI to enable 5620 SAM in-band management of the device by to configure a second trap destination and trap log on the device. See section 9.2 for information about in-band management. See the device documentation for configuration information.

4 If required, establish a route for in-band traffic. For example, to configure a static route or use OSPF. See chapter 22 for more information on static routes. See chapter 23 for more information about OSPF.

5 Configure the 5620 SAM to use in-band, out-of-band, or in-band and out-of-band polling for the device. A 5620 SAM mediation policy specifies the polling interval. See chapter 10 for information about mediation policies.

   a See Procedure 9-4 for 7450 ESS, 7705 SAR, 7710 SR, 7750 SR, and 7950 XRS polling configuration information.

   b See Procedure 9-5 for 7210 SAS polling configuration information.

   c See Procedure 9-6 for information about editing polling settings for multiple managed devices.

9.4 Device commissioning procedures

The following procedures describe how to commission devices that are natively-managed by the 5620 SAM except for the devices listed in Table 9-1. See section 8.1 for a list of all devices managed by the 5620 SAM. See the appropriate device documentation for information about using a device CLI.

Table 9-1 Location of device commissioning information

Device	Information location
1830 PSS	*1830 PSS-32/16 Installation and System Turn-Up Guide* *1830 PSS Engineering and Planning Tool User Guide* *1830 PSS DCN Planning and Engineering Guide (Photonic Applications)* *1830 PSS Commissioning and Power Balancing Tool User Guide*
5780 DSC	*5780 DSC User Guide*
7750 MG	*5620 SAM LTE EPC User Guide*
9471 WMM	Contact your ALU technical representative
eNodeB	Contact your ALU technical representative

Procedure 9-1 To commission a device for 5620 SAM management



Caution — Do not apply an SNMP log filter to the 5620 SAM SNMP log. The 5620 SAM cannot manage an NE that has an SNMP log filter applied to the log used by the 5620 SAM, which is typically log ID 98. In rare cases, Alcatel-Lucent may apply filters.

1 Open a console window on the device.

2 Enter the following command at the prompt to configure the system address of the device:

configure router interface "system" address *xxx.xxx.xxx.xxx/mask* ↵

where <*xxx.xxx.xxx.xxx*> is the system IP address
mask is the bit mask

3 Enter the following command at the prompt to enable Telnet:

configure system security telnet-server ↵

4 Enter the following command at the prompt to enable FTP:

configure system security ftp-server ↵

5 If required, enter the following command at the prompt to enable SSH2:

configure system security ssh version 2 ↵

6 Enter the following command at the prompt to enable console, FTP, and SNMP access for the appropriate user account on the device:

configure system security user *user_account* access console ftp snmp ↵

where *user_account* is the appropriate user account for Telnet, FTP, and SNMP access, for example, admin

7 If required, enter the following command at the prompt to enable hash encryption for passwords and authentication keys during device configuration save or list operations:

configure system security hash-control read-version *read-version* write-version *write-version* ↵

where
read-version is the version of encryption accepted during read operations, for example, 1, 2, or all to indicate that both are accepted
write-version is the version of encryption used during write operations, for example, 1 or 2

Version 1 encryption uses a simple key algorithm that generates the same character string each time it hashes a specific password or authentication key.

Version 2 encryption uses a more complex key algorithm that generates a different character string each time it hashes a specific password or authentication key.

8 Enter the following commands in sequence at the prompt to set the time zone and time:

configure system time zone *time_zone -offset_from_UCT* ↵

admin set-time *YYYY/MM/DD hh:mm:ss* ↵

where
time_zone is the appropriate time zone, for example, EST
offset_from_UCT is the offset, in hours, from Universal Co-ordinated Time, also known as Greenwich Mean Time, for example, if you specify EST, *offset_from_UCT* is -5, as EST lags UCT by five hours
YYYY/MM/DD hh:mm:ss is the current local time

9 If required, perform one of the following to enable a time protocol.

a Enter the following command at the prompt to enable NTP:

configure system time ntp server-address *server_IP_address* ↵

where
server_IP_address is the IP address of the SNTP server

b Enter the following command at the prompt to enable SNTP:

configure system time sntp server-address *server_IP_address* ↵

where
server_IP_address is the IP address of the SNTP server

10 Enter the following in sequence to enable the SNMPv2 engine and to configure an SNMP community:

configure system snmp no shutdown ↵

configure system snmp packet-size 9216 ↵

configure system security snmp community *community_name* rwa version both ↵

where *community_name* is the SNMPv2 community name



Note 1 — The command is used for the 5620 SAM write mediation policy. If you are using SNMPv2, you must use this mediation policy for read as well, or create another mediation policy that is also configured for rwa.

Note 2 — The SNMPv2 community string name rwa attributes must be enabled for the 5620 SAM to properly manage a device, even if the 5620 SAM is only used to monitor a network.

11 Enter the following commands in sequence at the prompt to ensure that the device uses persistent SNMP indexes:

bof persist on ↵

bof save ↵

12 Enter the following commands in sequence at the prompt to save the configuration changes and reboot the device:

```
admin save ↵

admin synchronize boot-env ↵

admin reboot now ↵
```

The device initializes with SNMP communication enabled.

13 Enter the following to clear the log ID and trap group ID:

```
configure log ↵

log-id 98 ↵

shutdown ↵

exit ↵

no log-id 98 ↵

no snmp-trap-group 98 ↵

exit all ↵
```

14 Use a 5620 SAM client to discover the device and to verify that the device configuration allows management of the device. See chapter 10 for information about device discovery. See "Network management configuration procedures" in the *5620 SAM System Administrator Guide* for information about performing device configuration backups.

15 Enter the following in sequence to verify the SNMP configuration:

```
configure log ↵

info ↵
```

The output is similar to the following:

```
snmp-trap-group 98

    description "5620sam"

    trap-target "xxx.xxx.xxx.xxx:mmm" address xxx.xxx.xxx.xxx
snmpv2c notify-community "privatetrap98"

    trap-target "yyy.yyy.yyy.yyy:nnn" address yyy.yyy.yyy.yyy
snmpv2c notify-community "privatetrap98"

exit

log-id 98

    from main security change

    to snmp 1024
```

```
exit
```

where

xxx.xxx.xxx.xxx is the IP address of the main server in a standalone 5620 SAM deployment, or one of the main servers in a redundant deployment

mmm is the SNMP port number

yyy.yyy.yyy.yyy is the IP address of the peer main server, if the 5620 SAM is deployed in a redundant configuration

nnn is the SNMP port number

Procedure 9-2 To commission an OmniSwitch for 5620 SAM management

See the appropriate OmniSwitch documentation for more information about the CLI command syntax and SNMP.



Note 1 — The 5620 SAM cannot discover an OmniSwitch that is configured with the factory default settings.

Note 2 — You must use a direct console port connection to access an OmniSwitch for the first time. All other management methods such as SNMP, Telnet, FTP, and HTTP, are disabled until you enable them.

1 Open a console window using a direct console port connection to the OmniSwitch.

2 Create a Loopback0 interface and assign an IP address to the interface by entering the following at the prompt:

`ip interface Loopback0 address` ***`xxx.xxx.xxx.xxx`*** ↵

where

xxx.xxx.xxx.xxx is the IP address of the interface



Note 1 — Loopback0 is the name assigned to an IP interface to identify an address that is used for network management purposes. The Loopback0 interface is not bound to any VLAN, therefore it always remains operationally active.

Note 2 — The Loopback0 interface name is case-sensitive. Ensure that you enter the name exactly as shown.

3 Enable SNMP sessions on the switch by entering the following at the prompt:

`aaa authentication snmp local` ↵

4 Enable FTP, Telnet, HTTP, or SSH sessions, if required, by entering the following at the prompt:

```
aaa authentication ftp local ↵

aaa authentication telnet local ↵

aaa authentication http local ↵

aaa authentication ssh local ↵
```

5 Perform one of the following to configure the required version of SNMP on the switch and the 5620 SAM:

The OmniSwitch default user, admin, does not have SNMP access. Before the 5620 SAM can discover an OmniSwitch, you must create at least one user on the switch with SNMP access.

a For SNMP v2c:

i Configure an SNMP v2 user by entering the following at the prompt:

```
user user_name password password no auth ↵
```

where
user_name is a username that corresponds to an SNMP v2 user who the 5620 SAM can identify; Alcatel-Lucent recommends that you use the name sam, which is the 5620 SAM default name
password is a password associated with the username; the password is between 8 and 47 characters



Note — If you need to use a different SNMPv2 default user name, create an SNMPv2 default user name on the 5620 SAM. See "To create a default SNMPv2 OmniSwitch user on a 5620 SAM system" in the *5620 SAM System Administrator Guide* for information about creating an SNMPv2 default user name.

ii Configure SNMP v2 trap forwarding to the 5620 SAM by entering the following at the prompt:

```
snmp station xxx.xxx.xxx.xxx v2 user_name ↵
```

where
xxx.xxx.xxx.xxx is the IP address of the 5620 SAM main server
user_name is the username that you created in step i

Trap forwarding configuration occurs automatically when the 5620 SAM discovers a switch and uses the default SNMP v2 user name sam or the user name configured, if any.

iii Configure an SNMP security level that allows the switch to accept all SNMP queries by entering the following at the prompt:

```
snmp security no security ↵
```

iv Configure an SNMP v2 community string by entering the following at the prompt:

snmp community map *community_string* user *user_name* ↵

where
community_string is the name of an SNMP v2 community string that the 5620 SAM can identify
user_name is the SNMP v2 username created in step i

v Create a mediation security policy on the 5620 SAM that uses a community string that matches the string created in step iv. See Procedure 10-4 for information about creating a mediation security policy.

vi Create a discovery rule on the 5620 SAM to discover the switch and reference the policy created in step v. See Procedure 10-7 for information about creating a discovery rule.

b For SNMP v3:

If you need to discover an OmniSwitch using SNMP v3 you must create an SNMP v3 user on the switch that matches an SNMP v3 user defined on the 5620 SAM.

i Configure an SNMP v3 user on the switch by entering the following at the prompt:

user *user_name* password *password security_level* ↵

where
user_name is a username that matches an SNMP v3 USM username configured on the 5620 SAM
password is a password associated with the username; the password is between 8 and 47 characters. The password is the plain text ASCII MD5/SHA authentication key and DES privacy key.
security_level is MD5, MD5 + DES, SHA, or SHA + DES

ii Configure SNMP v3 trap forwarding to the 5620 SAM by entering the following at the prompt:

snmp station *xxx.xxx.xxx.xxx* v3 *user_name* ↵

where
xxx.xxx.xxx.xxx is the IP address of the 5620 SAM main server
user_name is the username created in step i

Trap forwarding occurs automatically when the 5620 SAM discovers a device with a username that matches the SNMP v3 USM username specified in the 5620 SAM mediation policy.

iii Configure the SNMP v3 switch security option that you need by entering the following at the prompt:

snmp security *security_option* ↵

where *security_option* is one of the security options described in Table 9-2

Table 9-2 SNMP security options

Option	Description
no security	All SNMP queries are accepted.
authentication set	Includes: • SNPM v1 and v2 Gets • Non-authenticated v3 Gets and Get-Nexts • Authenticated v3 Sets, Gets, and Get-Nexts • Encrypted v3 Sets, Gets, and Get-Nexts
authentication all	Includes: • Authenticated v3 Sets, Gets, and Get-Nexts • Encrypted v3 Sets, Gets, and Get-Nexts
privacy set	Includes: • Authenticated v3 Gets and Get-Nexts • Encrypted v3 Sets, Gets, and Get-Nexts
privacy all (default)	Includes: • Encrypted v3 Sets, Gets, and Get-Nexts
traps only	Includes: • All SNMP requests are rejected

iv Create an SNMP v3 user on the 5620 SAM using the NE User Configuration manager. See "NE user and device security" in the *5620 SAM System Administrator Guide* for information about NE user configuration.

- Enable SNMP to give the SNMP v3 user SNMP access.
- Choose a username that matches the name created on the switch in step i.
- Choose the same SNMP v3 authentication protocol, privacy protocol, and password that is configured on the switch.

v Create an SNMP v3 mediation security policy. See Procedure 10-4 for information about configuring a mediation security policy.

- Choose the SNMP v3 (USM) security model option.
- Choose a username that matches the name created on the switch in step i.

vi Create a discovery rule that uses the mediation security policy created in step v. See Procedure 10-7 for information about creating discovery rules.

6 Use a 5620 SAM client to discover the switch and to verify that the switch configuration allows you to manage the switch.

Procedure 9-3 To configure the 5620 SAM SNMP trap sources

Perform this procedure to configure the sources of SNMP traps associated with log ID 98. If no SNMP log ID on a device matches the log ID in the 5620 SAM configuration, the 5620 SAM recreates the log ID and SNMP trap group on the device, which results in a single log file that receives traps from the following sources:

- main
- security—always included as an SNMP source
- change—supported by the 5620 SAM for the 7950 XRS and for the 7750 SR, Release 9.0 and later



Caution — This procedure requires a restart of each 5620 SAM main server, which is service-affecting. Perform this procedure only during a scheduled maintenance window.

1 If the 5620 SAM is deployed in a standalone configuration, go to step 6.

2 Perform the following steps to stop the standby main server.

i Log in to the standby main server station as the samadmin user.

ii Open a console window.

iii Enter the following to change to the server binary directory:

```
bash$ cd path/nms/bin ↵
```

where *path* is the main server installation location, typically /opt/5620sam/server

iv Enter the following to stop the main server application:

```
bash$ ./nmsserver.bash stop ↵
```

v Enter the following to display the main server status:

```
bash$ ./nmsserver.bash appserver_status ↵
```

The command displays a status message.

vi The main server is stopped when the command displays the following status message:

```
Application Server is stopped
```

If the command displays a different message, wait 5m and repeat step 2 v. Do not proceed to the next step until the server is stopped.

3 Perform steps 6 to 13 on the primary main server station.

4 Perform steps 6 to 13 on the standby main server station.

5 Go to step 14.

6 Log in to the main server station as the samadmin user.

7 Open the *path*/nms/config/nms-server.xml file using a plain-text editor

where *path* is the 5620 SAM server installation location, typically /opt/5620sam/server



Caution — Contact your Alcatel-Lucent technical support representative before you attempt to modify the nms-server.xml file. Modifying the nms-server.xml file can have serious consequences that can include service disruption.

8 Locate the following text section:

```
<snmp

ip="samserverIP"

port="nnn"

trapLogId="98"
```

where
samserverIP is the IP address of the 5620 SAM main server
nnn is the SNMP port number

This default configuration applies to traps from main, security, and change, if available.

9 Perform one of the following.

a To restrict the trap source to main only, add the following line:

```
logIdSourceBits="80"
```

b To restrict the trap source to main and change, add the following line:

```
logIdSourceBits="A0"
```

10 Save and close the nms-server.xml file.

11 Open a console window.

12 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

13 Enter the following to restart the main server:

```
bash$ ./nmsserver.bash force_restart ↵
```

The main server restarts, and the configuration change takes effect.

14 Close the console windows, as required.

Procedure 9-4 To configure polling for a 7450 ESS, 7705 SAR, 7710 SR, 7750 SR, or 7950 XRS

1 Choose Equipment or Routing from the navigation tree view selector. The managed devices are displayed.

2 Right-click on an icon that represents a 7750 SR, 7450 ESS, 7710 SR, 7705 SAR, or 7950 XRS and choose Properties. The Network Element (Edit) form opens with the General tab displayed.

3 Record the system IP address and the management IP address. Configure the Location and Current OLC State parameters, if required.

4 Click on the Polling tab.

5 Click on the General tab.

6 Specify whether scheduled polling is enabled or disabled using the Scheduled Polling parameter. Scheduled polling is configured using the Mediation configuration form. See Procedure 10-4 for more information.

7 Configure the Redundant Synchronization Mode parameter.

8 Verify that the Persistent SNMP Indices parameter is set to true to ensure persistent SNMP indices are used.

9 Configure the parameters:

- Primary DNS
- Secondary DNS
- Tertiary DNS
- DNS Domain
- Separate LI Administration
- LI Local Save Allowed



Note 1 — To configure LI parameters, you require LI user privileges.

Note 2 — To view LI configuration information, you need LI privileges. Right-click on a discovered device in the navigation tree and choose Properties from the contextual menu, and click on the LI Configuration Status tab.

10 View the read-only parameters to determine the current polling status:

- Resync Status indicates whether the last poll was successfully completed.
- Last Resync Start Time and Last Resync End Time indicate the start and finish of the last poll.
- Scheduled Resync Status indicates whether the last scheduled poll was successfully completed.
- Last Scheduled Resync Start Time and Last Scheduled Resync End Time indicate the start and finish of the last scheduled poll.

11 Click on the Management tab.

12 Configure the following parameters to specify an L3 management interface for in-band management, if required:

- L3 Management Interface
- Enable L3 Management Interface

13 Configure the following parameters:

- Active Management IP
- Auto Revert to Preferred
- Management IP Selection
- Primary Route Preference
- Secondary Route Preference



Note 1 — The Auto Revert to Preferred parameter is configurable when the Management IP Selection parameter is set to Out Of Band Preferred or In Band Preferred.

Note 2 — To avoid a communications outage between the 5620 SAM and managed NEs, the parameter settings in the Management Preference panel must match the parameter settings in the Notifications Preferred Management panel. See the Management IP Selection parameter description for more information.

Note 3 — If you want to transmit on in-band management on the 7705 SAR when both in-band and out-of-band management are both used, configure the Active Management IP, Auto Revert to Preferred, and Management IP Selection parameters as described in "7705 SAR management bandwidth".

14 Click on the OK button. A dialog box appears.

15 Click on the Yes button. The Network Element (Edit) form closes.

Procedure 9-5 To configure polling for a 7210 SAS

1 Choose Equipment or Routing from the navigation tree view selector. The managed devices are displayed.

2 Right-click on a device icon and choose Properties. The Network Element (Edit) form opens with the General tab displayed.

3 Record the system IP address and the management IP address. Configure the Location and Current OLC State parameters, if required.

4 Click on the Polling tab.

5 Specify whether scheduled polling is enabled or disabled using the Scheduled Polling parameter. Scheduled polling is configured using the Mediation configuration form. See Procedure 10-4 for more information.

6 Verify that the Persistent SNMP Indices parameter is set to true to ensure that persistent SNMP indices are used.

7 Configure the parameters in the Bof Configuration panel, if required:

- Primary DNS
- Secondary DNS
- Tertiary DNS
- DNS Domain

8 View the read-only parameters to determine the current polling status:

- Resync Status indicates whether the last poll was successfully completed.
- Last Resync Start Time and Last Resync End Time indicate the start and finish of the last poll.
- Scheduled Resync Status indicates whether the last scheduled poll was successfully completed.
- Last Scheduled Resync Start Time and Last Scheduled Resync End Time indicate the start and finish of the last scheduled poll.

9 Click on the Management tab.

10 On the In Band panel, configure the parameters:

- L3 Management Interface
- Enable L3 Management Interface

11 On the Management Preference panel, configure the parameters:

- Active Management IP
- Auto Revert to Preferred
- Management IP Selection



Note 1 — The Active Management IP, Auto Revert to Preferred, and Management IP Selection parameters are configurable only on the 7210 SAS-D 6F 4T and 7210 SAS-D 6F 4T ETR (Release 3.0 or later), the 7210 SAS-E, and the 7210 SAS-M. The 7210 SAS-X Release 3.0R2 or later supports a Management IP Selection value of Out of Band Preferred.

Note 2 — The Auto Revert to Preferred parameter is configurable when the Management IP Selection parameter is set to Out Of Band Preferred, In Band Preferred, or In Band Only.

12 On the Notifications Preferred panel, configure the following parameters:

- Primary Route Preference
- Secondary Route Preference

13 You can configure two uplinks in the BOF for port redundancy. If the image path and configuration file path are local, you do not need to configure the IP address and routing information for uplink A and uplink B. You can optionally obtain IP parameters using DHCP when you configure a value of 0 for the uplink port IP address. The DHCP server should be configured to provide the IP address and the default gateway information that is used to reach the server where the image and configuration files are stored.

14 Click on the 7210 BOF tab and on the Select button in the Uplink A panel to choose an uplink port. The Select Port - Uplink Bof Configuration search form opens.

15 Choose a port from the list and click on the OK button. The Select Port - Uplink Bof Configuration search form closes and the port name appears in the Uplink A panel.

16 Configure the following parameters in the Uplink A panel:

- IP Address
- Mask
- VLAN ID

17 Click on the Select button in the Uplink B panel to choose an uplink port. The Select Port - Uplink Bof Configuration search form opens.

18 Choose a port from the list and click on the OK button. The Select Port - Uplink Bof Configuration search form closes and the port name appears in the Uplink B panel.

19 Configure the following parameters in the Uplink B panel:

- IP Address
- Mask
- VLAN ID

20 Click on the Uplink Routes tab and on the Create button. The Uplink Route Configuration (Create) form opens.

21 Configure the following parameters:

- Uplink
- Route Destination
- Mask
- Next Hop

22 Click on the Apply button if you need to add more than one uplink route or the OK button if you only need to add one route. A dialog box appears.

23 Click on OK to save your configuration.

24 Repeat steps 21 to 23 to add another uplink route. You can add up to ten routes for each uplink.

25 Click on the OK button. A dialog box appears.

26 Click on the Yes button to confirm the action. The Network Element (Edit) form closes.

Procedure 9-6 To edit polling settings for multiple devices

You can use the list of managed devices from the Discovery Manager Resync Status tab to modify polling settings for a device or devices; for example, when you want to enable or disable polling on numerous managed devices.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form opens.

2 Click on the Resync Status tab.

3 Select a device or devices from the list.

4 Click on the Properties button. When you choose multiple devices, the Network Element (Multiple Instances) (Edit) form opens.

You can only configure those parameters that are common to all devices selected from the list.

5 Click on the Polling tab.

6 Enable or disable polling using the Scheduled Polling parameter.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button to confirm the action. The Network Element (Edit) form closes.

9.5 Workflow to commission GNEs

The following workflow describes the sequence of high-level tasks required to commission a GNE prior to discovery by the 5620 SAM.

1 Create a CLI script to enable trap forwarding to each main server in the 5620 SAM system. See the device documentation for information about configuring SNMP trap targets. See "CLI scripts" in the *5620 SAM Scripts and Templates Developer Guide* for information about using the 5620 SAM to create CLI scripts.

2 Create a CLI script to disable trap forwarding to each main server in the 5620 SAM system. See the device documentation for information about configuring SNMP trap targets.

3 Prepare the device for 5620 SAM discovery and management using a GNE profile. See Procedure 9-7 to prepare a device other than a 400 AWY or 9500 MSS-1c, and Procedure 9-9 to prepare a 400 AWY or 9500 MSS-1c.

4 If required, configure or modify a GNE alarm catalog for use with a GNE profile.

- Create a GNE alarm catalog; see Procedure 9-12.
- Create a transform function for the alarm catalog; see Procedure 9-13.
- Add an alarm mapping to the alarm catalog; see Procedure 9-14.

5 If required, enable the cross launch of a 9400 AWY or 9500 MSS-1c J-USM manager; see Procedure 9-17.

9.6 GNE commissioning procedures

The following procedures describe how to prepare a GNE for 5620 SAM management, and how to modify a GNE configuration after device discovery.

Procedure 9-7 To prepare a GNE for 5620 SAM management

Perform this procedure to prepare a GNE, which is typically a non-Alcatel-Lucent device, for 5620 SAM discovery and management.



Note 1 — To prepare a 9400 AWY or 9500 MSS-1c for 5620 SAM management, see Procedure 9-9.

Note 2 — See the *5620 SAM Management of OEM WT Products* application note on OLCS to obtain specific configuration information for the following GNEs:

- 9500 MPT-GC
- Radwin 2000
- Radwin 5000
- SUB 10 v320
- Siklu EH-1200

1 Preconfigure the device using a CLI. Perform the following steps.

i Enable FTP.

ii Enable Telnet.

iii Enable SNMP.

iv Configure at least one SNMPv1, SNMPv2c, or SNMPv3 community.

v Set the SNMP PDU size to 9216.

vi Enable persistent SNMP indexes.

2 Choose Administration→Generic NE Manager from the 5620 SAM main menu. The Generic NE Manager form opens.

3 Click on the Create button and choose Create Generic NE Profile. The Generic NE Profile (Create) form opens.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Generic NE Type
- Generic NE Category
- Sys Object ID
- Description
- Default Element Manager URL
- Alternate Element Manager
- Chassis MAC Object ID
- CLI Supported



Note 1 — The Sys Object ID parameter must begin with the following, which identifies the SMI enterprises subtree defined in RFC 1213:

.1.3.6.1.4.1

Note 2 — Do not enclose the Alternate Element Manager value in quotation marks; the 5620 SAM automatically encloses the value in quotation marks at run time.

Note 3 — To specify the target GNE IP address in the Default Element Manager URL or as a Default Alternate Element Manager command argument, use the %IP% keyword.

Note 4 — You cannot modify the Generic NE Type parameter after the GNE profile is created; you must delete the GNE profile and create a profile using the new Generic NE Type parameter value.

5 Click on the CLI Profile tab and configure the parameters:

- Command Prompt
- Max Number Of Sessions
- Telnet Port
- Pre Login Prompt
- Write Login Prompt
- Write Password Prompt
- Read Login Prompt
- Read Password Prompt
- Error Indicator
- Disable Paging Command
- Reset Command
- Login Timeout (seconds)
- Negotiation Delay (milliseconds)
- Execution Command Timeout (seconds)
- Login Prompt Optional
- Idle Session Warning Message
- Add CR to LF
- Drop Character After Invalid CR

6 Configure the following parameters if a login confirmation prompt appears:

- Enable Confirm Prompt
- Prompt
- Answer

The Prompt and Answer parameters are configurable when the Enable Confirm Prompt parameter is selected.

7 Configure the following parameters for a second level of login security, if required:

- Enable Second Login
- Enable Login Command
- Enable Login Prompt

The Enable Login Command and Enable Login Prompt parameters are configurable when the Enable Second Login parameter is selected.

8 To configure an interface for the GNE, perform the following steps.

i Click on the Interface Types tab.

ii Click on the Add button and use the Select Generic NE Interface Type form that opens to choose an interface type.

9 To associate one or more routing MIBs with the GNE profile, perform the following steps.



Note 1 — After you discover the device using the GNE profile, you can use the Routing view in the network navigation tree to view the discovered routing objects.

Note 2 — You must configure the GNE interface types before you associate a routing MIB with a GNE profile. Otherwise, you must perform a customized NE resync of all MIBs and select the Ignore Timestamps parameter.

i Click on the Routing MIBs tab.



Note — The Routing MIBs tab is dimmed if you do not have a valid 5650 CPAM license that has a third-party router quantity greater than zero. See "5650 CPAM routine system maintenance" in the *5650 CPAM User Guide* for information about 5650 CPAM licenses.

ii Click on the Add button. The Select Generic NE Routing MIB form is displayed.

iii Configure the filter and click on the Search button. The supported routing MIBs are listed.

iv Select one or more MIBs and click on the OK button. The MIBs are listed on the Generic NE Profile (Create) form.

10 Click on the Apply button. A dialog box appears.

11 Click on the Yes button. The form name changes to Generic NE Profile (Edit) and the Trap Configuration tab is enabled.

12 Click on the Trap Configuration tab.

13 Click on the Select button in the Trap Configuration Script panel and use the form that opens to choose a script. During device discovery, the 5620 SAM runs the script on the GNE to enable trap forwarding to the 5620 SAM.

14 Click on the Select button in the Trap De-Configuration Script panel and use the form that opens to choose a script. During device discovery, the 5620 SAM runs the script on the GNE to enable trap forwarding to the 5620 SAM.

15 Click on the Select button in the Alarm Catalogue panel and use the form that opens to choose an alarm catalog.

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The Generic NE Profile (Edit) form closes.

18 Close the Generic NE Manager form.

Procedure 9-8 To configure an alternate EMS for a specific GNE

Perform this procedure to specify an alternate EMS client application for a specific NE.



Note — The EMS that you specify overrides an EMS specified in the associated GNE profile.

1 Right-click on a GNE object in the network navigation tree and choose Properties from the contextual menu. The GNE properties form opens.

2 Configure the Alternate Element Manager parameter.



Note 1 — Do not enclose the Alternate Element Manager value in quotation marks; the 5620 SAM automatically encloses the value in quotation marks at run time.

Note 2 — To specify the target GNE IP address as an Alternate Element Manager command argument, use the %IP% keyword.

3 Click on the OK button. A dialog box appears.

4 Click on the Yes button. The GNE properties form closes.

Procedure 9-9 To prepare a 9400 AWY or 9500 MSS-1c for 5620 SAM management

5620 SAM management of a 9400 AWY or 9500 MSS-1c requires a GNE profile. Perform this procedure to prepare a 9400 AWY or 9500 MSS-1c for 5620 SAM discovery and management using a GNE profile.



Note — After you perform the procedure, each new profile is the default GNE profile for the device type.

1 Choose Administration→Mediation from the 5620 SAM main menu. The Mediation (Edit) form opens with the General tab displayed.

2 Record the Trap Destination Port value in the SNMP Trap panel.

3 Close the Mediation (Edit) form.

4 Register the 5620 SAM SNMP IP address with the 9400 AWY or 9500 MSS-1c. Perform the following steps.

- **i** Open the MCT or Multi-version NEtO.
- **ii** Open the required 9400 AWY or 9500 MSS-1c.
- **iii** Use the Trusted SNMP Manager option in the navigation tree to register the 5620 SAM IP address.
- **iv** Configure the Traps UDP Port for the 9400 AWY or 9500 MSS-1c using the Trap Destination Port value recorded in step 2.
- **v** Enter Network Manager Layer as the Type.
- **vi** Close the MCT or Multi-version NEtO.

5 Perform the following steps on each 5620 SAM main server station.

- **i** Log in to the main server station as the samadmin user.
- **ii** Open the *path*/nms/config/nms-server.xml file using a plain-text editor

  where *path* is the 5620 SAM server installation location, typically /opt/5620sam/server



Caution — Contact Alcatel-Lucent technical support before you attempt to modify the nms-server.xml file. Modifying the nms-server.xml file can have serious consequences that can include service disruption.

- **iii** Locate the line that begins with the following:

  ```
  systemGNEProfileNames=
  ```

iv Edit the line to read as one of the following, depending on the NE types that you want to manage:

- systemGNEProfileNames="MSS1c"
- systemGNEProfileNames="9400AWY"
- systemGNEProfileNames="MSS1c, 9400AWY"

v Save and close the nms-server.xml file.

6 If the 5620 SAM system is deployed in a redundant configuration, perform the following steps on the standby main server.

i Log in to the main server station as the samadmin user.

ii Open a console window.

iii Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

iv Enter the following to restart the main server:

```
bash$ ./nmsserver.bash force_restart ↵
```

The main server restarts and reads the updated configuration.

v Close the console window.

7 Perform the following steps on one of the following:

- the main server in a standalone deployment
- the primary main server in a redundant deployment

i Log in to the main server station as the samadmin user.

ii Open a console window.

iii Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

iv Enter the following:

```
bash$ ./nmsserver.bash read_config ↵
```

The main server reads the updated configuration and creates the GNE profiles.

v Close the console window.

8 Configure Discovery Manager for the required 9400 AWY or 9500 MSS-1c devices using the following:

- default SNMPv2 read-write access policy settings
- “SNMP-trap” as the SNMP community string

9 Ensure that a new group is created in the Equipment view of the network navigation tree, and that the group contains the required NEs.

10 To auto-populate the alarms catalog, perform the following steps.



Note — After you auto-populate an alarm catalog, the 5620 SAM processes the traps that are received from a GNE and raises alarms, as required; however, the 5620 SAM does not process the existing traps on a GNE.

i Choose Administration→Generic NE Manager from the 5620 SAM main menu. The Generic NE Manager form opens.

ii Click on the Search button. A list of GNE profiles is displayed.

iii Select the new GNE profile and click on the Properties button. The Generic NE Profile (Edit) form opens with the General tab displayed.

iv Click on the Populate Alarm Catalogue button. If the Populate Alarm Catalogue button is not present, click on the More Actions button and choose Populate Alarm Catalogue from the drop-down list. The 5620 SAM creates the alarm catalog.

v Click on the Trap Configuration tab.

vi Click on the Select button in the Alarm Catalogue panel and use the form that opens to specify an alarm catalog.

vii Click on the Interface tab.

viii Add each interface that is to send traps.

ix Generate new traps from the 9400 AWY or 9500 MSS-1c. The 5620 SAM alarm window displays the alarms.

Procedure 9-10 To modify a GNE profile

Perform this procedure to change a GNE profile configuration.

1 Choose Administration→Generic NE Manager from the 5620 SAM main menu. The Generic NE Manager form opens.

2 Choose Generic NE Profile (Generic NE) in the object drop-down list and click on the Search button. A list of GNE profiles is displayed.

3 Select a GNE profile in the list and click on the Properties button. The Generic NE Profile (Edit) form opens with the General tab displayed.

The following tabs contain configurable parameters:

- General—contains parameters that identify the GNE type
- CLI Profile—contains parameters that define the console window prompts and commands
- Trap Configuration—contains parameters that define the SNMP trap management configuration
- Interface Types—allows the association of multiple types of interfaces with the GNE profile



Caution — If you modify the list of interfaces on the Interface Types tab, you must resynchronize the entire GNE, as described in step 8.

4 Modify the parameters for the GNE profile, as required.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Generic NE Profile (Edit) form closes.

7 Close the Generic NE Manager form.

8 If you modify the list of interfaces on the Interface Types tab, perform the following steps.

i Right-click on the GNE in the 5620 SAM topology map and choose Resync→Customized Resync from the contextual menu. The Resync Site(s) form opens with the Resync Options panel displayed.

ii Click on the Next button. The Force Resync panel is displayed.

iii Select the Ignore Timestamps parameter.

iv Click on the Finish button. The 5620 SAM resynchronizes the GNE.

v Close the Resync Site(s) form.

Procedure 9-11 To delete a GNE profile



Note 1 — You cannot delete a GNE profile that is associated with a managed GNE. You must unmanage the GNEs associated with a GNE profile before you can delete the profile.

Note 2 — You cannot delete a GNE profile when a GNE associated with the profile is a target of a CLI script. See “Script management” in the *5620 SAM Scripts and Templates Developer Guide* for more information about CLI script management.

1 Unmanage and delete the GNEs that are managed using the GNE profile. See chapter 10 for more information.

2 Choose Administration→Generic NE Manager from the 5620 SAM main menu. The Generic NE Manager form opens.

3 Choose Generic NE Profile (Generic NE) in the object drop-down list and click on the Search button. A list of GNE profiles is displayed.

4 Select a profile in the list and click on the Delete button. A dialog box appears.

5 Click on the Yes button. The 5620 SAM deletes the GNE profile.

6 Close the Generic NE Manager form.

Procedure 9-12 To create a GNE alarm catalog

Perform this procedure to create an alarm catalog for use with a GNE profile.

1 Choose Administration→Generic NE Manager from the 5620 SAM main menu. The Generic NE Manager form opens.

2 Click on the Create button and choose Create Generic NE Alarm Catalogue. The Generic NE Alarm Catalogue (Create) form opens.

3 Configure the parameters:

- Catalogue Name
- Description
- Version

4 Perform steps 3 to 18 of Procedure 9-13 to create a transform function for the catalog, if required.

5 Click on the Mappings tab.

6 Click on the Create button to create a raising alarm mapping. The Generic NE Alarm Mapping (Create) form opens.

7 Configure the following parameters:

- Trap OID
- Trap Name
- Administrative State
- FDN Extension
- Additional Text
- Use Default Additional Text

8 Perform one of the following using the parameters in the Alarm Name panel.

a Specify a static alarm name by configuring the Alarm Name parameter.

b Specify a dynamic alarm name. Perform the following steps.

i Select the Specify Transform Function parameter.

ii Click on the Select button beside the Varbind Transform Function parameter. The Select Transform Function form opens.

iii Select a transform function in the list and click on the OK button. The Select Transform Function form closes, and the transform function name is displayed on the Generic NE Alarm Mapping (Create) form.

iv Configure the Varbind Position parameter.

9 Perform one of the following using the parameters in the Probable Cause panel.

a Specify a static probable cause. Perform the following steps.

i Click on the Select button beside the Probable Cause parameter. The Select Property form opens with a list of probable causes displayed.

ii Select a probable cause in the list and click on the OK button. The probable cause is displayed on the Generic NE Alarm Mapping (Create) form.

b Specify a dynamic probable cause. Perform the following steps.

i Select the Specify Transform Function parameter.

ii Click on the Select button beside the Varbind Transform Function parameter. The Select Transform Function form opens.

iii Select a transform function in the list and click on the OK button. The Select Transform Function form closes, and the transform function name is displayed on the Generic NE Alarm Mapping (Create) form.

iv Configure the Varbind Position parameter.

10 Perform one of the following using the parameters in the Severity panel.

a Specify a static severity by configuring the Severity parameter.

b Specify a dynamic severity. Perform the following steps.



Note — When you specify the use of a transform function for the alarm severity, the Mapping Type changes to Raising/Clearing. You cannot create a clearing mapping for this type of mapping; you must use a transform function to clear an alarm when the alarm severity is defined using a transform function.

i Select the Specify Transform Function parameter.

ii Click on the Select button beside the Varbind Transform Function parameter. The Select Transform Function form opens.

iii Select a transform function in the list and click on the OK button. The Select Transform Function form closes, and the transform function name is displayed on the Generic NE Alarm Mapping (Create) form.

iv Configure the Varbind Position parameter.

11 Configure the varbind positions for specific objects on a GNE in the Alarmed Object panel:

- System Address Varbind Position
- Interface Index Varbind Position



Note — In order to configure the System Address Varbind Position and Interface Index Varbind Position parameters, you must set the Alarm Name parameter to GNE MTIE Alarm.

12 Click on the OK button. A dialog box appears.

13 Click on the OK button. The Generic NE Alarm Mapping (Create) form closes, and the new alarm mapping is listed on the Generic NE Alarm Catalogue (Create) form.

14 Repeat steps 6 to 13 to create an additional raising alarm mapping, if required.

15 If you do not need to create a clearing alarm mapping, go to step 25.

16 To create a clearing alarm mapping, select a raising alarm mapping in the list and click on the Create Clearing button. The Generic NE Alarm Mapping (Create) form opens.



Note 1 — A raising alarm mapping is indicated by the word Raising in the Mapping Type list column.

Note 2 — You can create a clearing alarm mapping only when the corresponding raising alarm is in the same alarm catalog.

Note 3 — You can associate a clearing alarm mapping with only one raising alarm mapping.

Note 4 — You cannot create a clearing mapping for a mapping that uses a transform function to define the alarm severity; you must use a transform function to clear an alarm when the alarm severity is defined using a transform function.

17 Configure the parameters:

- Trap OID
- Trap Name
- Administrative State
- FDN Extension
- Additional Text
- Use Default Additional Text



Note 1 — A static clearing alarm mapping inherits the following values from the associated raising alarm:

- Alarm Name—must match raising alarm Alarm Name
- Probable Cause—must match raising alarm Probable Cause
- FDN Extension—resulting text string must match text string generated by raising alarm mapping
- Additional Text—resulting text string must match text string generated by raising alarm mapping

See Procedure 9-15 for information about modifying the Alarm Name or Probable Cause value.

Note 2 — The explicit FDN Extension and Additional Text values can differ from the values in the raising mapping, but the generated text strings must match. For example, if the object name is in varbind 2 of the raising trap and in varbind 3 of the clearing trap, the parameter values name different varbinds but the script output is identical.

Note 3 — The alarm severity in a clearing alarm mapping is set to Cleared and cannot be changed.

18 Perform the following steps to specify a dynamic alarm name, if required, using the parameters in the Alarm Name panel.

i Select the Specify Transform Function parameter.

ii Click on the Select button beside the Varbind Transform Function parameter. The Select Transform Function form opens.

iii Select a transform function in the list and click on the OK button. The Select Transform Function form closes, and the transform function name is displayed on the Generic NE Alarm Mapping (Create) form.

iv Configure the Varbind Position parameter.

19 Perform the following steps to specify a dynamic probable cause, if required, using the parameters in the Probable Cause panel.

i Select the Specify Transform Function parameter.

ii Click on the Select button beside the Varbind Transform Function parameter. The Select Transform Function form opens.

iii Select a transform function in the list and click on the OK button. The Select Transform Function form closes, and the transform function name is displayed on the Generic NE Alarm Mapping (Create) form.

iv Configure the Varbind Position parameter.

20 Click on the OK button. A dialog box appears.

21 Click on the OK button. The Generic NE Alarm Mapping (Create) form closes, and the new alarm mapping is listed on the Generic NE Alarm Catalogue (Create) form.

22 Repeat steps 16 to 21 to create and additional clearing alarm mapping, if required.

23 Click on the OK button. A dialog box appears.

24 Click on the OK button. The Generic NE Alarm Mapping (Edit) form closes.

25 Click on the OK button. A dialog box appears.

26 Click on the Yes button. The Generic NE Alarm Catalogue (Edit) form closes.

27 Close the Generic NE Manager form.

Procedure 9-13 To create a transform function for a GNE alarm catalog

1 Choose Administration→Generic NE Manager from the 5620 SAM main menu. The Generic NE Manager form opens.

2 Click on the Create button and choose Create Generic NE Alarm Catalogue. The Generic NE Alarm Catalogue (Create) form opens.

3 Click on the Transform Functions tab.

4 Click on the Create button. The Generic NE Alarm Transform Function (Create) form opens.

5 Configure the parameters:

- Transform Function Name
- Out Value Type
- Specify Default Out Value

6 If you enable the Specify Default Out Value parameter, click on the Select button beside the Default Out Value parameter. The Select Property form opens. Otherwise, go to step 8.

7 Select a value in the list and click on the OK button. The Select Property form closes, and the value is displayed on the Generic NE Alarm Transform Function (Create) form.

8 Click on the Pairs tab.

9 Click on the Create button. The Pair (Create) form opens.

10 Configure the In Value parameter.

11 Click on the Select button beside the Out Value parameter. The Select Property form opens.

12 Select a value in the list and click on the OK button. The value is displayed on the Pair (Create) form.

13 Click on the OK button. A dialog box appears.

14 Click on the OK button. The Pair (Create) form closes, and the value pair is listed on the Generic NE Alarm Transform Function (Create) form.

15 Repeat steps 9 to 14 to add another value pair, if required.

16 Click on the OK button. A dialog box appears.

17 Click on the OK button. The Generic NE Alarm Transform Function (Create) form closes, and the transform function is listed on the Generic NE Alarm Catalogue (Edit) form.

18 Repeat steps 4 to 17 to create another transform function, if required.

19 Click on the OK button. A dialog box appears.

20 Click on the Yes button. The Generic NE Alarm Catalogue (Edit) form closes.

21 Close the Generic NE Manager form.

Procedure 9-14 To add an alarm mapping to a GNE alarm catalog



Note — A modification to a GNE alarm catalog takes effect immediately after you commit the change.

1 Choose Administration→Generic NE Manager from the 5620 SAM main menu. The Generic NE Manager form opens.

2 Choose Generic NE Alarm Catalogue (Trap to Alarm Mapper) in the object drop-down list and click on the Search button. A list of GNE alarm catalogs is displayed.

3 Select an alarm catalog in the list and click on the Properties button. The Generic NE Alarm Catalogue (Edit) form opens with the General tab displayed.

4 Configure the Description and Version parameters, if required.

5 Perform steps 5 to 27 in Procedure 9-12.

Procedure 9-15 To modify or delete a GNE alarm mapping

1 Choose Administration→Generic NE Manager from the 5620 SAM main menu. The Generic NE Manager form opens.

2 Choose Generic NE Alarm Catalogue (Trap to Alarm Mapper) in the object drop-down list and click on the Search button. A list of GNE alarm catalogs is displayed.

3 Select an alarm catalog in the list and click on the Properties button. The Generic NE Alarm Catalogue (Edit) form opens with the General tab displayed.

4 Click on the Mappings tab.

5 Perform one of the following.

a Modify the mapping. Perform the following steps.



Note — A modification to a GNE alarm mapping takes effect immediately after you commit the change.

i Select a mapping in the list and click on the Properties button.The Generic NE Alarm Mapping (Edit) form opens.



Note — To change the Alarm Name value in a raising alarm mapping and in the associated clearing alarm mapping, you must do one of the following:

- Configure the parameter in each mapping simultaneously by selecting both mappings before you click on the Properties button.
- Configure the parameter in one mapping at a time and commit the changes to the catalog only after both mappings are modified.

ii Configure the following parameters:

- Trap Name
- Administrative State
- Alarm Name
- Severity
- FDN Extension
- Additional Text
- Use Default Additional Text

iii Click on the Select button beside the Probable Cause parameter. The Select Property - Generic NE Alarm Mapping form opens with a list of probable causes displayed.

iv Select a probable cause in the list and click on the OK button. The probable cause is displayed on the Generic NE Alarm Mapping form.

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The Generic NE Alarm Mapping (Create) form closes.

b Delete the mapping. Perform the following steps.



Note — When you delete a GNE raising alarm mapping, the associated clearing mapping is also deleted.

i Select a mapping in the list and click on the Delete button. A dialog box appears.

ii Click on the OK button. The 5620 SAM deletes the GNE alarm mapping.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The Generic NE Alarm Catalogue (Edit) form closes, and the Generic NE Manager form reappears.

8 Close the Generic NE Manager form.

Procedure 9-16 To delete a GNE alarm catalog



Note 1 — You cannot delete an alarm catalog that is associated with a GNE profile. You must remove the alarm catalog from each associated GNE profile before you can delete the catalog.

Note 2 — When you delete a GNE alarm catalog, you delete the alarm mappings that the catalog contains.

1 Choose Administration→Generic NE Manager from the 5620 SAM main menu. The Generic NE Manager form opens.

2 Choose Generic NE Alarm Catalogue (Trap to Alarm Mapper) in the object drop-down list and click on the Search button. A list of GNE alarm catalogs is displayed.

3 Select an alarm catalog in the list and click on the Properties button. The Generic NE Alarm Catalogue (Edit) form opens with the General tab displayed.

4 Click on the Generic NE Profiles tab. The tab lists the GNE profiles to which the alarm catalog is assigned.

5 If no profiles are listed, go to step 8.

6 Perform the following steps to remove a profile association.

i Select a profile in the list and click on the Properties button. The Generic NE Profile (Edit) form opens with the General tab displayed.

ii Click on the Trap Configuration tab.

iii Click on the Clear button in the Alarm Catalogue panel. The Catalogue Name value is removed from the form.

iv Click on the OK button. A dialog box appears.

v Click on the Yes button. The Generic NE Profile (Edit) form closes, and the Generic NE Alarm Catalogue (Edit) form reappears.

7 Repeat step 6 for each listed profile.

8 Close the Generic NE Alarm Catalogue (Edit) form. The Generic NE Manager form reappears.

9 Select the alarm catalog in the list and click on the Delete button. A dialog box appears.

10 Click on the Yes button. The 5620 SAM deletes the GNE alarm catalog.

11 Close the Generic NE Manager form.

Procedure 9-17 To cross launch the 9400 AWY or 9500 MSS-1c J-USM manager

Perform this procedure to enable the cross launch of a Java-based EMS/craft terminal.

1 Perform Procedure 9-7 to discover the 9400 AWY or 9500 MSS-1c GNE.

2 Perform one of the following to specify the NEtO directory path:



Note — Option B is the preferred method.

a Configure the NEtO directory path on each NE. Perform the following steps.

i Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

ii Right-click on the 9400 AWY or MSS-1c GNE and choose Properties. The Network Element (Edit) form opens with the General tab displayed.

iii Specify the directory name in the External EMS field.

b Configure and use the same NEtO directory path for all devices that are discovered using a discovery rule. Perform the following steps.

i Open the Discovery Manager form and choose the Discovery Rules tab.

ii Select the discovery rule for the NEs and click on the Properties button. The Topology Discovery Rule (Edit) form opens with the General tab displayed.

iii Specify the NEtO directory name in the Default External EMS field



Note — To cross launch a 9400 AWY NE, retain the NEtO software directory in your 5620 SAM client and remove any spaces in the NEtO directory path.

3 Click on the OK button. A dialog box appears.

4 Click on the Yes button. The Network Element (Edit) form closes.

5 Right-click on the GNE and choose External Element Manager from the contextual menu. The MCT/NEtO is launched.

10 — Device discovery

10.1 Device discovery overview *10-2*

10.2 Resynchronization of NEs *10-8*

10.3 Mediation and SNMP MIBs *10-9*

10.4 SSH security *10-9*

10.5 Server resource management *10-11*

10.6 SNMP event notification policies *10-11*

10.7 Workflow to discover network devices *10-12*

10.8 Device discovery procedures *10-14*

10.1 Device discovery overview

The 5620 SAM discovers devices using SNMP and stores the device properties in the 5620 SAM database. To discover one or more devices, you use the 5620 SAM Discovery Manager to create a discovery rule, and then scan the network for devices according to the IP addresses or address ranges specified in the rules.

A discovery rule contains one or more rule elements that specify which devices or subnets are to be included in, or excluded from, the discovery process. For example, you can configure one rule element to discover a subnet and another to exclude specific IP addresses from the subnet.

Note — The 5620 SAM does not attempt to discover tests or test suites that are configured locally on a device, for example, using a CLI.

When the system IP address, also called the system ID, is used to discover a device, the management is in-band. When the management IP address is used to discover a device, the management is out-of-band. See chapter 9 for information about in-band and out-of-band management.

Note — If you need to change the system name of a device, you must unmanage and delete the device from the 5620 SAM before you change the name, and then rediscover the device, See Procedures 10-16 and 10-18 for information about unmanaging and deleting devices.

A device can be in one of the following management states:

- managed—the 5620 SAM manages the device
- not managed—an operator has unmanaged the formerly managed device; the management information is removed from the 5620 SAM database
- suspended—an operator has suspended management of the device; see "Suspending device management" in this section for more information

Suspending device management

When you need to exclude a device from 5620 SAM management but do not want to lose the 5620 SAM information about the device, for example, during a maintenance period that may generate an exceptional number of SNMP traps, you can use a GUI or OSS client to suspend the management of the device.

Caution — When you suspend the management of a device, the 5620 SAM raises a critical alarm against the device.

When you suspend management of a device, the 5620 SAM removes the 5620 SAM trap target entries from the device configuration, and the following operations are subsequently blocked:

- SNMP deployment and trap handling; all traps from the device are dropped
- NETCONF deployments and event subscriptions

- statistics collection
- automated FTP and other file transfers
- GUI or OSS client configuration of device parameters; a configuration attempt results in a failed deployment
- scheduled and periodic operations that the 5620 SAM initiates, such as the following:
  - connectivity checks
  - resynchronizations
  - device configuration backups
  - device software upgrades
  - OAM test and test suite execution

Note 1 — You cannot suspend the management of a device while a software upgrade or configuration backup is in progress on the device.

Note 2 — If you attempt to modify an OAM test or test suite that is deployed to a suspended NE, the 5620 SAM raises an alarm. The alarm does not automatically clear when the NE is remanaged.

You can use the 5620 SAM to perform the following on a suspended device:

- open a Telnet or SSH CLI session
- execute CLI scripts
- open an FTP session
- configure 5620 SAM parameters that affect the device management but are not deployed, such as the in-band or out-of-band management preferences

As shown in Figure 10-1, when a device is suspended, the device icons in the network navigation tree and physical topology map are colored purple. The following icons are also colored purple to indicate that at least one device is suspended:

- parent group icon in the network navigation tree Equipment and Routing views
- parent group icon in the physical topology map

Note — The group icon colors are prioritized; when a group contains one or more unreachable NEs and one or more suspended NEs, the group icon is colored red.

Figure 10-1 GUI representation of suspended device

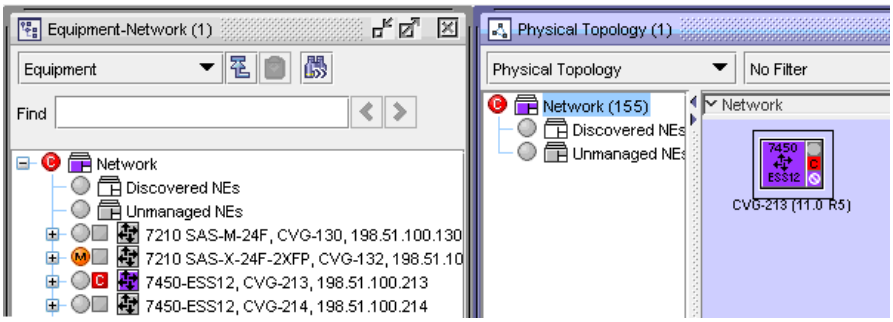


Figure 10-1 shows The Network equipment group. When a suspended device is in a group other than the Network group, only the lower right corner of the Network group icon is colored purple.

When you return a suspended device to the managed state, the 5620 SAM rediscovers the device to capture events such as device reboots or software release changes, and initiates a full device resynchronization based on the response to a trap sequence ID check.

Note — The 5620 SAM also checks the device management parameters to adapt to a switch from one type of management to another, for example, from in-band to out-of-band.

Unmanaging and deleting devices

Using the 5620 SAM to unmanage a device excludes the device from the managed network, but a reference to the device remains in the 5620 SAM discovery system. The unmanage function may be used for unusual conditions such as when the 5620 SAM requires a complete refresh of device data because of data corruption. Unmanaging a device results in a loss of management data for the selected device, which includes, but is not limited to, the following:

- object names and descriptions
- statistics
- alarms
- physical links
- policies
- script results
- scheduled activities
- device configuration backups

Deleting a device results in the complete loss of management data for the device and completely removes the device from the managed network.

Caution — Unmanaging or deleting a device results in the loss of all historical 5670 RAM AA statistics for the device.

Post-discovery actions

In a discovery rule, you can create and specify a post-discovery action to perform on the successfully discovered NEs included in the rule. The 5620 SAM performs the post-discovery action automatically at the end of rule execution.

A post-discovery action requires a 5620 SAM control script that manages the auto-configuration actions performed on discovered NEs.

For example, an operator specifies a control script as a post-discovery action in a discovery rule for a subnet. The control script co-ordinates the execution of device-specific child control scripts. The child control scripts call XML API scripts that each configure a group of discovered NEs, such as aggregation ring or IP backhaul NEs. After the 5620 SAM executes the discovery rule, it invokes the control script to auto-configure the successfully discovered NEs in the subnet.



Note — Because a post-discovery action is intended to be autonomous, the 5620 SAM displays an error message and halts a post-discovery action that requires user interaction.

See "Script management" in the *5620 SAM Scripts and Templates Developer Guide* for information about creating control scripts, and for information about viewing example scripts.

From the Managed State tab of the Discovery Manager form, you can do the following:

- List the post-discovery action associated with each managed NE.
- View the status of the script execution as it occurs.
- View the script run result.

The Node Discovery Control form of an NE displays additional information and allows post-discovery action management. See Procedure 10-9 for more information.

The following conditions apply to post-discovery actions.

- The 5620 SAM performs no logic validation of the associated scripts.
- Deletion of the associated control script is blocked.
- After a discovery rule runs, the action is not automatically executed on new NEs that are added to the rule. To execute the action on the new NEs, you must rescan the network using the rule.
- An action is performed on an NE only when the Full Resync Status of the NE is Full Resync Done.
- If a device fails discovery, the action is not performed, and the script execution status is Not Executed. Resynchronization of the NE does not invoke the script or change the execution status.
- If the control script execution fails, an alarm is raised.
- After a post-discovery action is performed on an NE:
  - Unmanaging and remanaging the NE has no effect.
  - Deleting and rediscovering the NE causes the action to be performed on the NE.

SNMP management

Simple Network Management Protocol, or SNMP, is an application-layer protocol that provides a message format to facilitate communication between SNMP managers and agents. SNMP provides a standard framework for NE monitoring and management from a central location.

An SNMP manager controls and monitors the activities of network hosts that use SNMP. An SNMP manager uses a get operation to obtain a value from an SNMP agent, and uses a set operation to store a value in the agent. The manager uses definitions from a management information base, or MIB, to perform operations on the managed device, for example, retrieving data values, replying to requests, and processing SNMP notifications called traps.

SNMPv1 and SNMPv2c provide no security, authentication, or encryption. Without authentication, an unauthorized user is able to perform SNMP network management functions and eavesdrop on management information as it passes from one system to another.

SNMPv3 requires that an authentication and encryption method such as SSH is assigned to each user for validation by the NE. SNMPv3 authentication and encryption enable an NE to validate the system that issues an SNMP message and to determine whether another system has tampered with the message.

For information about device-specific SNMP support, see the SNMP chapter of the appropriate *System Management Guide* for the device. For information about SSH security, see section 10.4.

IPv6 discovery

The 5620 SAM supports the discovery of devices that use IPv6 in-band or out-of-band management IP addresses. In order for the 5620 SAM to discover and manage a device that uses IPv6, the device must have an IPv6 address on the management port, system interface, or both. The 5620 SAM main server must also be given an IPv6 address during installation.



Note — To manage 7750 SR, 7710 SR, 7450 ESS, 7950 XRS devices using IPv6, the device must also be configured with an IPv4 address on the management port for out-of-band management, or an IPv4 address on the system interface for in-band management.

The IP version that the 5620 SAM uses to discover a device is specified in each discovery rule. If the 5620 SAM discovers both IPv4 and IPv6 addresses on the system interface of a device, it discovers the device using the address that corresponds to the IP version specified in the discovery rule.

Discovery and SNMP packet size

The network infrastructure carrying traffic between the 5620 SAM Servers/Auxiliaries and the managed NEs must support fragmentation and reassembly of the UDP packets for NEs that have an SNMP PDU size greater than the MTU configured for the network path between the NE and 5620 SAM. The 7210 SAS, 7450 ESS, 7705 SAR, 7710 SR, 7750 MG, 7750 SR, and 7950 XRS require an SNMP PDU size of 9216 bytes to be configured and fragmentation support is required in the network path between the 5620 SAM and the NE.

Consider the following:

- When an intermediate network device receives SNMP traffic, it must be able to process fragmentation of packets. If the SNMP packet exceeds the MTU size of the intermediate device, and the device does not support fragmentation of packets, the packets may be dropped and device discovery may fail.
- Verify that data payloads of the SNMP PDU size can travel from the managed devices to the 5620 SAM by using a CLI to ping the IP address of the 5620 SAM main server, using a packet size of the configured SNMP PDU. See "Packet size and fragmentation issues" in the *5620 SAM Troubleshooting Guide* for information about using traceroute and ping to verify packet transport.

9500 MPR radio link discovery and management

The 5620 SAM supports N x (1+x) radio [x = 0, 1] link discovery. To enable 9500 MPR radio link discovery and management, the 5620 SAM requires connectivity between the 9500 MPR NE radio ports, as shown in Figure 10-2 and described in Table 10-1.

Figure 10-2 Connectivity example for 9500 MPR radio link discovery and management

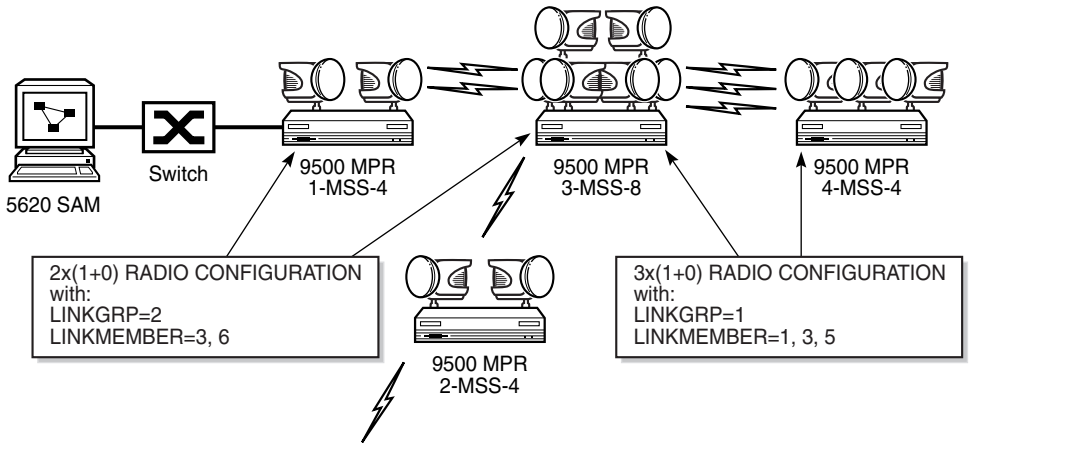


Table 10-1 Connectivity parameter details

	1-MMS-4	2-MSS-4	3-MSS-8	4-MSS-4
2-MSS-4	PPPRF Enabled LinkID (as assigned)	—	PPPRF Enabled LinkID (as assigned)	—
3-MSS-8	PPPRF Enabled LinkID (23, 23) PPPRF Disabled LinkID (26, 26)	PPPRF Enabled LinkID (as assigned)	—	PPPRF Enabled LinkID (11, 11) PPPRF Disabled LinkID (13, 13) PPPRF Disabled LinkID (15, 15)

To discover multiple radio links, you must provision the radio ports on the 9500 MPR based on the following criteria.

1 Only one radio port can have PPPRF enabled. The far endpoint on the same link must have the same configuration as the first endpoint. PPPRF should be disabled on both endpoints for the second and any subsequent radio links.

2 LinkID requirements include:

- The LinkID must be enabled for all of the port members of the configuration that have the same LINKGRP, and a different LINKMEMBER that matches the far endpoint.
- Expected and Sent values must be equal (for example, 11, 11 or 13, 13).
- For a multiple Nx(1+x) radio configurations on the same NE, the LINKGRP must be unique without overlapping (for example, 1 and 2).
- LinkID should be formatted as LINKGRP:LINKMEMBER in a hexidecimal format where LINKGRP is the first character and LINKMEMBER are the members.
- Any mismatch between the LinkID at the link level (for example, Send is not equal to Expected) mutes the radio connection (MPT case).

3 As a requirement for the first radio link to be discovered, the remote address must be configured at both endpoints. For subsequent links, alarms cannot be present on the radio port.

4 When Radio Link Aggregation is enabled for any of the radio links between two 9500 MPRs, all radio links must belong to the same LAG.

10.2 Resynchronization of NEs

The Resync contextual menu option for an object specifies that SNMP MIB and CLI information bases for the object are reread to resynchronize them with the 5620 SAM database. When you choose the Resync option at the NE level, you can choose to resynchronize all MIBs or perform a customized resynchronization. When you choose to resynchronize all MIBs, the color of the device object in the navigation tree is yellow during the resynchronization. See Procedure 10-7 for more information about performing NE resynchronizations.

The Resync Status tab of the Discovery Manager form displays the following resynchronization attributes for each managed NE; the attributes are updated after an attempted resynchronization of all MIBs, but not after a customized resynchronization attempt:

- Resync Status
- Last Resync Start Time
- Last Resync End Time
- Scheduled Resync Status
- Last Scheduled Resync Start Time
- Last Scheduled Resync End Time

The Resync Status value is one of the following:

- Full Resync Done—a resynchronization has successfully completed
- Full Resync Failed—a resynchronization attempt has failed

  Full Resync Failed does not indicate that the SNMP agent on the NE is unreachable; if the agent is unreachable, an alarm is raised against the NE and the NE icon color changes to red. When the agent is again reachable, the alarm clears and the NE icon color changes to green.
- In Progress—a resynchronization is in progress
- Not Attempted—no resynchronization has been requested
- Requested—the resynchronization request is queued for processing.

The Scheduled Resync Status value is one of the following:

- In Progress—a resynchronization is in progress
- Not Attempted—no resynchronization has been requested
- Scheduled Resync Done—a resynchronization has successfully completed
- Scheduled Resync Failed—a resynchronization attempt has failed

10.3 Mediation and SNMP MIBs

A 5620 SAM mediation policy defines the interval at which the 5620 SAM polls NEs for SNMP MIB configuration changes. You can use the Mediation and MIB Entry Policy forms to view the information in an SNMP MIB. See Procedure 10-4 for more information.

You can use the 5620 SAM client GUI to list the contents of the device MIBs that the current 5620 SAM system supports. The list includes the following information:

- the MIB name
- the MIB version; the 5620 SAM software may support multiple MIB versions
- the OID of a MIB entry
- the MIB entry name
- the 5620 SAM polling interval for a MIB or MIB entry

See Procedure 10-24 for information about listing and saving SNMP MIB information.

10.4 SSH security

SSH is a protocol that provides secure file transfer and file system access between the 5620 SAM, and managed NEs. SSH version 2, or SSH2, is enabled by default on many devices.

SSH2 supports the use of public/private encryption-key pairs to perform authentication based on public key cryptography. A public/private key pair is generated on an NE. The private key is stored locally on the NE, and the public key is specific to SSH2 clients and persists in the 5620 SAM for future communication with the SSH2 server on the NE. The public key is used to verify that the client is connecting to the correct SSH2 server.

An SSH2 server identifies itself to a client by sending a message that is signed with the private key of the server. The 5620 SAM uses the public key of the SSH2 server to authenticate the identity of the server.

SSH2 host key management

An NE sends an SSH2 host key on the first attempt of the 5620 SAM to make an SSH2 connection. The 5620 SAM automatically accepts the public key fingerprint and stores it locally. After the first connection, the local copy of the fingerprint is used for server authentication during subsequent sessions.

If a different host key is sent by the same NE in a subsequent session, the connection is rejected and the 5620 SAM raises an alarm. If the user verifies that the host key of the SSH2 NE has been changed in a legitimate manner, for example, when the SSH server is rebooted and host key persistence is not configured, the user can manually accept the key by removing the mismatched host key entry from the SSH2 known host manager of the 5620 SAM. This removes the SSH2 fingerprint from the 5620 SAM database. Connections are then accepted from the NE until the SSH server is again rebooted.



Note — By default, SSH host keys do not persist in the 7210 SAS, 7450 ESS, 7705 SAR, 7710 SR, 7750 SR, and 7950 XRS.

Alcatel-Lucent recommends that you configure the host key persistence on an SSH2 NE to retain the public key fingerprint across reboots. If public key persistence is not enabled, a 5620 SAM operator must manually accept a new key and remove an alarm each time a connection attempt is made after the NE reboots.

SSH2 and device CLI sessions

When SSH2 for CLI sessions is enabled in the mediation policy of an SSH2-capable device, SSH2 instead of Telnet is used for each CLI session.

SSH1 is used only in SSH CLI sessions on NEs that do not support SSH2.

SSH2 and script management

When SSH2 for CLI sessions is enabled in the mediation policy of an SSH2-capable device, SSH2 is used instead of Telnet for each script execution session.

SSH1 is used only in SSH CLI sessions on NEs that do not support SSH2.

SSH2 and secure file transfers

When secure file transfers are specified in the mediation policy of an SSH2-capable device, SCP is used instead of FTP for backups, restores, software upgrades, and statistics collection.

10.5 Server resource management

The 5620 SAM supports the grouping of NEs by network function for increased SNMP mediation efficiency.

Resource allocation is automatically configured during 5620 SAM installation and network discovery based on the available system resources, and the numbers and types of NEs that are to be managed. The resource group to which an NE belongs is initially determined by the device type. The following are the 5620 SAM NE resource groups and the default device assignments:

- global—for 5620 SAM tasks that are not associated with NEs
- default—for NEs that do not belong to a specific resource group
- core—for 7450 ESS, 7750 SR, and 7950 XRS devices
- middle—for 7210 SAS, 7710 SR, and 7705 SAR devices
- edge—for OmniSwitch and similar devices
- GNE—for other network devices

The 5620 SAM logs the system load of each resource group at regular intervals. An Alcatel-Lucent support representative can monitor system resource usage, determine whether the current resource allocation is appropriate, and reconfigure resource management, if required.



Caution — Only a qualified Alcatel-Lucent support representative can assess or configure 5620 SAM server resource management. Contact Alcatel-Lucent technical support for more information.

10.6 SNMP event notification policies

To reduce the 5620 SAM processing load associated with SNMP events, you can configure a policy that specifies which SNMP traps the 5620 SAM processes. An event notification policy acts as a filter that enables or disables the processing of specific SNMP traps for a specific NE type and release.

A 5620 SAM operator with an admin or operations scope of command role and write access permission to the policy package can create an event notification policy using the Mediation form. The 5620 SAM assigns a default event notification policy to an NE during initial device discovery. A 5620 SAM operator can create and apply a policy that specifies which traps to process and which to ignore. 5620 SAM processing is enabled for all supported traps in the default policy. See Procedure 10-10 for information about configuring an event notification policy.

The following conditions apply to event notification policies:

- After an NE upgrade, the 5620 SAM processes the new traps generated by the upgraded NE. A 5620 SAM administrator must ensure that the event notification policies that are in effect before an NE upgrade are correctly configured, and must modify them after the upgrade to silenced new traps, if required.
- 5620 SAM software upgrades do not affect existing event notification policies.



Caution — The 5620 SAM relies on certain SNMP notifications to verify network management activities. Before you configure an event notification policy, consult an Alcatel-Lucent support representative to ensure that you do not disable the processing of traps that are vital to 5620 SAM operation.

SNMP statistics that include the number of ignored traps for an NE are available from the Statistics tab of the NE properties form.

10.7 Workflow to discover network devices

The following workflow describes the sequence of high-level tasks required to discover network devices. The following must be true before the 5620 SAM can discover a device.

- Each Alcatel-Lucent device is commissioned; see chapter 9 for commissioning information.
- Each non-Alcatel-Lucent device has a GNE profile; see chapter 9 for information.

1 Using a CLI, ensure that each device you want to discover and manage using SNMPv3 has a unique engine ID. See Procedure 10-1 for information.

2 If required, perform the following steps to configure SSH2 security.

i Enable SSH2 on the device. See Procedure 10-2 for information.

ii Configure and start an SSH server on the device. See the appropriate device documentation for SSH configuration information.



Note — A 7705 SAR may become temporarily unreachable after you enable SSH and start the SSH server on the device.

iii If the device supports SSH2 host key persistence, use Telnet to enable the function on the device. See Procedure 10-3 for information.

3 Create a mediation policy. If you want to use SSH2 for mediation, ensure that you enable SSH2 for CLI sessions and secure file transfers. See Procedure 10-4 for information.



Note — If you specify the use of SNMPv3 in the policy, you must enable SSH2 in the policy.

4 Configure the control scripts and XML API scripts for post-discovery actions, as required. See the *5620 SAM Scripts and Templates Developer Guide* for information about control and XML API script configuration.

5 Create post-discovery actions to associate with discovery rules, as required. See Procedure 10-5.



Note — You can also create a post-discovery action during discovery rule creation.

6 Create discovery rules, as required. See Procedure 10-6.



Note — If you want to use SSH2, specify the created SSH2 mediation policy for read and write access in the discovery rule.

7 Discover devices, as required. See Procedure 10-7.

8 If the discovery rule includes a post-discovery action, perform the following, as required.

- View the script execution status for the action. See Procedure 10-8.
- For an NE with a script execution status of Failed, clear the script execution status and manually execute the script. See Procedure 10-9.

9 As required, create event notification policies. See Procedure 10-10 for information.

10 As required, assign event notification policies to NEs. See Procedure 10-11 for information.

11 As required, manage device discovery by performing one or more of the following using the procedures in this chapter.

a Edit discovery rules and rule elements. See Procedure 10-12 for information.

b Enable or disable discovery rules. See Procedure 10-13 for information.

c Delete discovery rules. See Procedure 10-14 for information.

d Rescan the network using a discovery rule. See Procedure 10-15 for information.

e Manage, unmanage, or delete managed devices. See Procedures 10-16, 10-17, and 10-18 for information.

f Synchronize NEs with the 5620 SAM database. See Procedure 10-19 for information.

g Monitor the acceptance and rejection of SSH2 host keys using the 5620 SAM SSH2 Known Host Key Manager. See Procedures 10-20 and 10-21 for information.

h Switch from non-secure to secure mediation for one or more devices. See Procedures 10-22 and 10-23 for information.

i List and save SNMP MIB information. See Procedure 10-24 for information.

10.8 Device discovery procedures

Use the following procedures to configure device discovery and mediation.

Procedure 10-1 To configure SNMPv3 on a device

Perform this procedure to enable SNMPv3 on a device. SNMPv3 provides user-based security. The access granted is restricted to the scope of the configured users and groups.

If you are configuring an NE for LI, you must create a second access group. See chapter 28 for information about creating an LI user and access group.

1 Open a CLI session on the device.

2 Enter the following commands in the order shown to create a read-write-notify group for general SNMP mediation on the managed device:

```
configure system security snmp ↵

access group "snmpv3_groupname" security-model usm security-level
privacy read "iso" write "iso" notify "iso" ↵
```

where
snmpv3_groupname is the name that is being assigned to the SNMP group



Note — For 9500 MPR SNMPv3 passwords see the 9500 MPR documentation.

3 If mediation of VPRN objects is required, enter the following command to create a read-write-notify group for this purpose on the managed device:

access group "*snmpv3_groupname*" security-model usm security-level privacy context vprn prefix read "vprn-view" write "vprn-view" notify "iso" ↵

where
snmpv3_groupname is the name that is being assigned to the SNMP group

4 Enter the following command to exit SNMP group configuration.

exit ↵

5 Enter the following command to obtain the SNMP engine ID of the device.

show system info ↵

The SNMP engine ID is displayed as SNMP Engine ID.

6 Generate an MD5 or SHA authentication key, and DES privacy keys, using the password2key utility on a 5620 SAM client or server station.

- MD5 and SHA authentication keys are used to create an encrypted authentication password for users.
- DES privacy keys are used to encrypt the entire SNMP packet, for additional security.



Note — The length of a generated key is determined by the authentication method. MD5 keys are 32-character strings. SHA keys are 40-character strings.

i Log in to the 5620 SAM client or server station.



Note 1 — If you are using the password2key utility on a RHEL or Solaris 5620 SAM main server station, you must log in as the samadmin user.

Note 2 — If you are using the password2key utility on a 5620 SAM client station, you must log in as a local administrator, or as the user who installed the client.

ii Open a console window.

iii Navigate to the *install_directory*/nms/bin directory

where *install_directory* is the 5620 SAM installation location, typically /opt/5620sam/server or /opt/5620sam/client on RHEL and Solaris, and C:\5620sam\client on Windows

iv Enter the following to create an MD5 or SHA authentication key.

nmsclient.bat password2key *method password engine_ID* ↵

where
method is the type of encryption algorithm used to generate the authentication key, either MD5 or SHA
password is the ASCII password string used to generate the authentication key for the SNMPv3 user, for example, yoga
engine_ID is the SNMP engine ID obtained in step 5

The SHA authentication key generated from this example is 60210e3d2bfa7e02682262df9c5de400b9c3322b.

v Enter the following to create an MD5 or SHA DES privacy key.

nmsclient.bat password2key *method password engine_ID* ↵

where
method is the type of encryption algorithm used to generate the DES privacy key, either MD5 or SHA
password is the ASCII password string used to generate the DES privacy key, for example, happy
engine_ID is the SNMP engine ID obtained in step 5

The DES privacy key generated from this example is 4088f4ef966b8d1ebe54b8d841a5f76806c374ec.

vi If your security model requires unique keys for each managed device, repeat steps 6iv and 6v for each set of keys to be generated.

vii Store the generated keys.

7 Using the keys generated in step 6, create an SNMPv3 user on the managed device.

i Enter the following sequence of commands at the prompt:

```
configure system security user snmpv3_username ↵

access snmp ↵

snmp ↵

authentication method authentication_key privacy des-key
DES_privacy_key ↵

group snmpv3_groupname ↵

exit all ↵
```

where
snmpv3_username is the name being assigned to the SNMPv3 user
snmpv3_groupname is the name of the new SNMP user group
method is sha or md5, depending on the authentication method used
authentication_key is the SHA or MD5 authentication key generated in step 6
DES_privacy_key is the DES privacy key generated in step 6



Note — A DES privacy key is 32 characters long. If SHA encryption, which produces a 40-character key, is used to generate the DES privacy key in step 6, you must provide only the first 32 characters of the key, as shown in the following example that uses the key values from step 6:

```
authentication sha
60210e3d2bfa7e02682262df9c5de400b9c3322b privacy des
4088f4ef966b8d1ebe54b8d841a5f768 ↵
```

ii Enter the following command at the prompt to save the configuration changes.

```
admin save ↵
```

The device is now ready to be managed using SNMPv3. To enable device management by the 5620 SAM, you must do the following:

- Create an SNMPv3 user using the 5620 SAM NE user configuration manager. See "NE user and device security" in the *5620 SAM System Administrator Guide* for information about creating and configuring NE users. You must specify the following for each user:
  - Give the user SNMP access.
  - Enter the same User Name as the user name created earlier in this procedure.
  - On the SNMPv3 tab, select SHA as the authentication protocol and DES as the privacy protocol.
  - Type the appropriate ASCII password used to generate the MD5 or SHA authentication key, and DES privacy key, in step 6; for example, yoga and happy.
- Create a new SNMPv3 mediation security policy, as described in Procedure 10-4. Specify the following:
  - the SNMPv3 USM security model
  - the SNMP user name created earlier in this procedure
- Create one or more discovery rules that use the new SNMPv3 mediation policy.

8 Close the CLI session.

Procedure 10-2 To verify that SSH2 is enabled on a device

Perform this procedure to verify that SSH2 is enabled on a device, and to enable SSH2 on the device, if required.

1 Open a CLI session on the device.

2 Run the following CLI command to see whether SSH2 is enabled:

```
show system security ssh ↵
```

3 If required, enter the following command at the prompt to enable SSH2:

```
configure system security ssh version 2 ↵
```

4 Close the CLI session.

Procedure 10-3 To enable SSH host key persistence on a device

Perform this procedure to enable the persistence of the server host key on a 7210 SAS, 7450 ESS, 7750 SR, 7705 SAR, 7710 SR, or 7950 XRS. For other devices, see the user documentation for information about configuring SSH2 host key persistence.

1 Open a CLI session on the device.

2 Enter the following at the prompt to disable the SSH server:

```
configure system security ssh server-shutdown ↵
```

3 Enter the following at the prompt to enable host key persistence:

```
configure system security ssh preserve-key ↵
```

4 Enter the following at the prompt to enable the SSH server:

```
configure system security ssh no server-shutdown ↵
```

5 Enter the following at the prompt to verify that the preserve-key function is enabled on the server:

```
show system security ssh ↵
```

6 Close the CLI session.

Procedure 10-4 To configure NE mediation

Perform this procedure to configure the 5620 SAM to poll NEs at regular intervals. To configure LI mediation, see Procedure 28-7.

1 Choose Administration→Mediation from the 5620 SAM main menu. The Mediation (Edit) form opens with the General tab displayed.

2 Configure the parameters:

- Polling Synchronization Time
- Polling Admin State
- Discovery Rule Scan Interval



Note — Polling and scanning use system resources, and can increase the amount of management traffic. Consider your network needs and network management domain capabilities before you perform this procedure.

3 Configure MIB polling intervals for different managed devices, as required.

i Click on the MIB Entry Policies tab. A list of MIBs appears, organized by the product name of the device that supports the MIB.

ii Configure the search filter, if required, and click on the Search button. A list of MIB entry policies that match the search criteria is displayed.

iii Choose one or more MIBs from the list.

iv Click on the Properties button. The MIB Entry Policy (Edit) form opens with the General tab displayed.

v Configure the parameters:

- Polling Interval
- Administrative State
- Number of Varbind per PDU
- Use GETBULK to Walk SNMP Table



Caution — Changing the Number of Varbind per PDU parameter value may affect the time required for subsequent NE resynchronizations and degrade 5620 SAM server performance. Do not configure the parameter without contacting Alcatel-Lucent technical support.

vi Click on the OK button. A dialog box appears.

vii Click on the Yes button. The MIB Entry Policy (Edit) form closes and the Mediation (Edit) form reappears.

4 Click on the Ping tab to define how the management IP addresses of devices are checked using a ping. Each managed device may provide one or more of the following three IP addresses, each of which can be scheduled to be pinged, as configured during discovery rule creation:

- the system IP address, called an in-band management interface
- the management IP address on the management port, called an out-of-band management interface
- the IP address of the standby Control card, also called a CPM



Note — When the device does not have one or two of the IP addresses, for example, there is no CPM IP address, ensure that you create a ping policy that does not have its schedule enabled. This allows the assignment of an inactive ping policy during discovery configuration. See Procedure 10-7 for information.

i Click on the Ping tab.

ii Click on the Create button to create a new ping policy, or click on the Properties button to change an existing ping policy.

The Management Ping Policy (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Auto-Assign ID
- Policy ID
- Displayed Name
- Ping Command Timeout (seconds)
- Schedule Enabled
- Ping Interval (minutes)
- Ping Interval (seconds)

You must enable scheduling for the default ping policy to be performed. When scheduling is not enabled, and a managed device is not reachable, management connection alarms may not be raised.

The destination interface of the ping is determined during the creation of discovery rules for devices. You can also perform an unscheduled ping from the Managed State tab of the Discovery Manager configuration form. See Procedure 10-7 for more information.

iv Click on the OK button to save the changes. A warning dialog box appears.

You can view management connection alarms from the NE properties form of the managed device that was pinged. For example, from the Discovery Manager form, click on the Resync Status tab. Choose a device from the list and click on the Properties button. From the NE properties form, click on the Faults tab to view the alarms.

v Click on the OK button.

5 Create or modify a statistics MIB policy to determine how often the 5620 SAM polls the managed device MIBs for statistics. See "Performance statistics collection" in the *5620 SAM Statistics Management Guide* for information about statistics collection.

6 Click on the Mediation Security tab.

i Click on the Create button to create a new SNMP mediation security policy, or choose an existing policy and click on the Properties button to modify the policy. The Mediation Policy form opens with the General tab displayed.



Note — To configure SNMPv3 security, you must preconfigure the 5620 SAM server and the managed devices. See Procedure 10-1 for information.

ii Configure the general mediation parameters:

- Policy ID
- Auto-Assign ID
- Displayed Name
- Security Model
- Timeout (milliseconds)
- Retry
- Port
- Community String



Note 1 — The recommended value for Timeout (milliseconds) parameter specifying the SNMP timeout value for polling or deployment requests between the 5620 SAM and the 1830 PSS device is 60000.

Note 2 — The recommended value for Retry parameter specifying the number of retries for SNMP polling or deployment requests between the 5620 SAM and the 1830 PSS device is 2.

Note 3 — The Community String value must match the community string value on the managed device.

Note 4 — The default Community String for the trap access mediation policy on the 9500 MPR and 9500 MPRe is SNMP-trap.

Note 5 — The Community String for the 1830 PSS device access mediation policy should be set to nms_snmp.

iii Configure the parameters in the CLI and File Transfer panels:

- Communication Protocol
- User Name
- User Password

  You must also enter the User Password parameter value in the Confirm Password parameter field.
- File Transfer Type



Note 1 — If you choose Secure as the File Transfer Type parameter value, you must set the Communication Protocol parameter to SSH2.

Note 2 — To configure SSH2 you must enable SSH2 and host key persistence on the SSH server of the device. See section 10.4 for information about configuring SSH2.

Note 3 — If you choose SSH2 as the Communication Protocol, the User Name and User Password parameters must be the user name and password for the SSH server.

Note 4 — The default User Name and User Password for FTP access on the 9500 MPR and 9500 MPRe, is ftp.

7 If you choose SSH2 as the Communication Protocol value in step 6 iii, configure the SSH2 Server Port parameter.

8 Perform one of the following.

a If you choose FTP as the File Transfer Type value in step 6 iii, configure the parameters in the FTP panel:

- User Name
- User Password
  You must also enter the User Password parameter value in the Confirm Password parameter field.
- Connect Timeout (sec)
- Read Timeout (sec)



Note — The default ftp User Name and Password is “ftp” for the 9500 MPR read/write access Mediation policy.

b If you choose Secure as the File Transfer Type value in step 6 iii, configure the parameters in the Secure FTP panel:

- Connect Timeout (sec)
- Read Timeout (sec)

See chapter 9 for information about enabling FTP access for a device user account.

9 If you set the Security Model parameter to SNMPv3 (USM), assign a user profile that is configured with the SNMPv3 authentication and privacy parameters, as described in Procedure 10-1.

i Click on the Select button to view a list of configured users. The Select Site User For SNMP Access form opens.

ii Select a user from the list and click on the OK button. The user name is displayed on the Mediation Security form.

iii Click on the Properties button to open the configuration form for the user and view or modify the SNMPv3 security settings, if required.

10 See the *5620 SAM LTE EPC User Guide* and *5620 SAM LTE RAN User Guide* for information about how to configure the NETCONF parameters for the eNodeB and the 9471 WMM.

11 Click on the OK button. A dialog box appears.

12 Click on the OK button. The Mediation Policy form closes and the Mediation (Edit) form reappears.

13 Close the Mediation (Edit) form.

Procedure 10-5 To configure a post-discovery action

Perform this procedure to create a post-discovery action that you can associate with one or more discovery rules.



Note — You can also create a post-discovery action during discovery rule creation.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens with the Discovery Rules tab displayed.

2 Click on the Post Discovery Actions tab.

3 Click on the Create button. The Post Discovery Action (Create) form opens.

4 Configure the parameters:

- Name
- Description

5 Click on the Select button beside the Control Script Name parameter and use the list form that opens to choose a control script.

6 Click on the Select button beside the Control Script Instance Name parameter and use the list form that opens to choose a control script instance.

7 Click on the OK button. A dialog box appears.

8 Click on the OK button. The Post Discovery Action (Create) form closes, and the post-discovery action is listed on the Discovery Manager form.

9 Click on the OK button. A dialog box appears.

10 Click on the Yes button. The Discovery Manager form closes.

Procedure 10-6 To configure a discovery rule

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens with the Discovery Rules tab displayed.

2 Click on the Create button to create a new discovery rule. The Create Discovery Rule - Specify General Attributes step form opens.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Description
- Administrative State
- OLC State
- Revert OLC State when discovery completes
- Management Protocol
- Default External EMS



Note — When you close the Discovery Manager form, the 5620 SAM scans the network using the discovery rule, if the Administrative State parameter of the discovery rule is set to Up.

4 Click on the Select button beside the Group Name parameter. The Select Discovery Group - Topology Discovery Rule form opens with a list of topology groups displayed.

5 Select a topology group from the list and click on the OK button. The topology group name is displayed on the Create Discovery Rule step form.



Note 1 — If the selected topology group reaches the maximum element limit, any additional discovered NEs are automatically added to the Discovered NEs group.

Note 2 — The Discovered NEs Group Name cannot be chosen when configuring a Discovery Rule for an EM system. See Procedure 6-28 for information about creating unique topology groups.

6 Click the Next button. The Create Discovery Rule - Add Rule Elements form opens.

7 Click on the Create button to add a new rule element. The Topology Discovery Rule Element (Create) form opens.

8 Configure the parameters:

- IP Address
- Mask Bits
- Usage

9 Click on the OK button. The Topology Discovery Rule Element (Create) form closes and a dialog box appears.

10 Click on the OK button.

11 Repeat steps 7 to 10 to create an additional rule element, if required.

12 Click on the Next button. The Add Auto Discovery Rule Elements ACL form opens.

13 Click on the Create button. The Auto Discovery Rule Element ACL (Create) form opens.

14 Configure the parameters:

- System ID
- Action

15 Click on the OK button. The Auto Discovery Rule Element ACL (Create) form closes.

16 Repeat steps 13 to 15 to create an additional automatic discovery rule element, if required.

17 Click on the Next button. The Create Discovery Rule - Configure Mediation Security form opens.

18 Click on the Select button in each of the following panels, as required, and use the Configure Mediation Security form to specify the mediation security policies for the discovery rule.

- Read Access Mediation Policy
- Write Access Mediation Policy
- Trap Access Mediation Policy



Note 1 — If you do not specify a policy, the default policy is applied.

Note 2 — A 9400 AWY or 9500 MSS-1c discovery rule requires the default SNMPv2 read and write access policies.

19 Click on the Next button. The Create Discovery Rule - Configure Management Ping Policy form opens.

20 Click on the Select button in each of the following panels, as required, and use the Configure Management Ping Policy form to specify the ping policies for the discovery rule.

- Out Of Band Management Interface Ping
- In Band Management Interface Ping
- Standby CPM Ping



Note 1 — If you do not specify a policy, the default policy is applied.

Note 2 — Management ping policies are created using the Mediation configuration form. These are the policies applied during discovery rule creation. You must apply a ping policy even to interfaces that do not exist. When there is no interface, you must choose a ping policy that has its Schedule Enabled parameter set to disabled.

For example, if there is no standby CPM or out-of-band management IP address, specify a ping policy that has the Schedule Enabled parameter set to disabled for the nonexistent management and standby CPM interfaces. In this example, a ping policy with the Schedule Enabled parameter enabled is required for the in-band interface that does exist. See Procedure 10-4 for information about creating ping policies.

21 Click on the Next button. The Create Discovery Rule - Configure MIB Statistics Policy form opens with the default MIB statistics policy displayed.

22 Click on the Select button to choose a different MIB statistics policy, if required. The Configure MIB Statistics Policy form opens. Select a MIB statistics policy in the list and click on the OK button.

23 Click on the Next button. The Create Discovery Rule - Add Discovered Routers to Span(s) form opens.

24 Click on the Add button to specify a span of control for the new NE contained in the discovery rule. If you do not specify a span, the default span is applied.



Note — New devices added to a span from a discovery rule are added explicitly to the span.

When a discovered NE group is part of a user-defined span, new devices that are discovered using the discovery rule are automatically added to the span.

25 Click on the Next button. The Create Discovery Rule - Configure Backup Policy form opens with the default backup policy displayed.

26 If required, click on the Select button and use the Select Backup Policy form to choose a different backup policy.

27 Click on the Next button. The Create Discovery Rule - Add NE Self Config Policies form opens.



Note — This form requires configuration only for eNodeB discovery. See "Self-configuration and discovery" in the *5620 SAM LTE RAN User Guide* for information about eNodeB discovery.

28 Click on the Next button. The Create Discovery Rule - Add EM Systems form opens.

29 Click on the Create button. The EM System (Create) form opens with the General tab displayed.

30 Configure the parameters:

- ID
- Auto-Assign ID
- Element Manager System Name
- Description
- Administrative State

31 Click on the Element Managers tab.

32 Click on the Create button. The Element Manager (Create) form opens.



Note 1 — If the EM system being discovered is an OMC-RAN, only space and underscore are supported characters for NE names. Any other special characters will be replaced by an underscore.

Note 2 — After discovering an EM system, the system should be opened and its administrative state set to Up in order to enable the connection to the 5620 SAM. A maximum of four EM Systems may have their administrative state set to Up at any time within the 5620 SAM.

Note 3 — A manual resync must be performed in order for alarms from an EM system to display in the 5620 SAM or Supervision web portal. This does not apply to the EM system (NEtO) for 9500 MPR devices; alarms are aggregated automatically provided the Trap Access Mediation policy in the Discovery step form is configured.

Note 4 — The 5620 SAM is able to manage 10 000 alarms per EM system. When this limit is reached, a critical alarm is raised and new incoming alarms are deleted. When the alarm counter for the EM System drops to 9000, the critical alarm is cleared and the 5620 SAM performs an alarm resynchronization on the EM system.

33 Configure the parameters:

- Host Name
- Server IP Address
- Server Port Number
- User Name
- Password
- Confirm Password

34 Click on the OK button. The Element Manager (Create) form closes and the EM System (Create) form reappears.

35 Click on the OK button. The EM System (Create) form closes and the Create Discovery Rule - Add EM Systems form reappears.

36 Click on the Next button. The Create Discovery Rule - Add Post Discovery Action form opens.

37 To specify a post-discovery action, perform one of the following.

a Click on the Select button and use the list form that opens to associate an existing post-discovery action with the discovery rule.

b Create a post-discovery action to associate with the discovery rule. Perform the following steps.

i Click on the Select button. The Select Post Discovery Action form opens.

ii Click on the Create button. The Post Discovery Action (Create) form opens.

iii Configure the parameters:

- Name
- Description

iv Click on the Select button beside the Control Script Name parameter and use the list form that opens to choose a control script.

v Click on the Select button beside the Control Script Instance Name parameter and use the list form that opens to choose a control script instance.

vi Click on the OK button. The Post Discovery Action (Create) form closes, and the post-discovery action is listed on the Select Post Discovery Action form.

vii Select the new post-discovery action and click on the OK button. The new post-discovery action is associated with the discovery rule.

38 Click on the Finish button. The Create Discovery Rule step form closes and a dialog box appears.

39 Click on the OK button. The Discovery Manager form reappears.



Note — When you close the Discovery Manager form, the 5620 SAM scans the network using the discovery rule, if the Administrative State parameter of the discovery rule is set to Up.

40 Click on the OK button. A dialog box appears.

41 Click on the Yes button. The Discovery Manager form closes.

Procedure 10-7 To discover devices

Perform this procedure to complete the following tasks:

- Ping the managed devices to test connectivity
- Locate managed devices on a topology map
- Discover devices by scanning the network according to discovery rules
- Resynchronize NEs and the 5620 SAM database
- Check the discovery, management, and synchronization status of a device



Note 1 — SNMP parameters must be correctly specified using CLI on the managed devices. Contact your Alcatel-Lucent support representative or see chapter 9 for information about using CLI to commission devices before managing them.

Note 2 — Ensure that in-band and out-of-band management are correctly configured to discover devices, as described in chapter 9.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens with the Discovery Rules tab displayed.

2 Click on the Apply button to discover devices by scanning the network as specified by a discovery rule.

New or modified discovery rules are saved. The 5620 SAM discovers devices by scanning the network as specified by the discovery rules. After a device is discovered, the 5620 SAM server sets the device in a managed state and adds the device elements to the 5620 SAM database.

Discovery rules that are disabled or shut down are not applied.

3 Verify that the device is discovered and is managed by the 5620 SAM by clicking on the Managed State tab on the Discovery Manager form. A list of managed devices opens.

The management state of the device is displayed in the Site State column. Managed is the default state. If the device is unmanaged, select the device from the list and click on the Manage button.

4 From the Managed State tab, you can also perform management IP address pings to ensure connectivity to all managed devices. Do not ping devices without an interface.

5 From the Managed State tab, you can locate the device in a topology map.

i Click on one or multiple managed devices in the list.

ii Click on the Navigate button. A drop-down menu opens that lists the map view options.

iii Select an option. The *topology_view* (Navigate) form appears showing the selected network objects.



Note — Only managed devices that are not in the Discovered NEs group can be located. If the selected managed devices do not all belong to the same group on the map, then only the managed devices of one of the groups is located. Unmanaged devices cannot be located.

6 Verify that the device configuration has been reconciled with the 5620 SAM database contents, by clicking on the Resync Status tab. The Resync Status tab displays the operation status of the last full resync. See section 10.2 for more information.

To initiate manual device reconciliation, select one or more devices in the list and click on the Resync button.

If the reconciliation fails:

- View faults that are associated with a device by double-clicking on the device in the Discovery Manager form and clicking on the Faults tab in the form that opens.
- Check the SNMP security parameters on a device using the CLI.
- Check the 5620 SAM mediation settings.

Successfully discovered NEs appear in the 5620 SAM navigation tree.

7 From the Resync Status tab, you can locate the device in a topology map.

i Click on one or more resynchronized devices in the list.

ii Click on the Navigate button. A drop-down menu opens that lists the map view options.

iii Select an option. The *topology_view* (Navigate) form appears showing the selected network objects.



Note — Only devices located outside the discovery group can be located. If the selected devices do not all belong to the same group on the map, then only the devices of one of the groups is located.

8 Close the Discovery Manager form.

Procedure 10-8 To view the post-discovery action execution status

Perform this procedure to view the script execution status of a post-discovery action associated with a discovery rule.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens with the Discovery Rules tab displayed.

2 Click on the Managed State tab.

3 View the entries in the Script Execution Status column. The possible values are:

- unspecified—post-discovery action not specified in discovery rule
- Pending—post-discovery action execution awaits discovery completion
- Not Executed—control script not executed
- In Progress—control script execution in progress
- Successful—control script execution completed without failure indication
- Failed—control script execution unsuccessful
- Cleared—Failed state manually cleared

4 For each NE that has a Failed entry, perform the following steps to view the script execution result.

i Click on the Show Results button. The Results form for the NE opens.

ii Click on the Search button. A list of script results is displayed.

iii Select a result in the list and click on the Properties button. The View Result form opens. The form displays information such as the script name, version, run time, and execution status.

iv View the information to determine the required corrective action.

v If required, perform the following steps to export the result information to a file.

- Choose File→Export from the View Result form main menu, or click on the Export icon. The Export form opens.
- Navigate to the location in which you want to save the file, and enter a filename in the File Name field.
- Click on the Export button. The result text is saved in the specified file.



Note — You can also export a script result to a file using the Export button on the Results form for the NE.

5 Close the View Result form.

6 To delete a result, perform the following steps.

i Select the result on the Results form and click on the Delete button. A dialog box appears.

ii Click on the Yes button. The result is deleted.

7 Close the Results form.

8 Close the Discovery Manager form.

Procedure 10-9 To manage a post-discovery action failure on an NE

Perform this procedure to do the following:

- reset the script execution status for an NE
- manually run the post-discovery action script against the NE

This action may be required after the script associated with a post-discovery action fails and the cause of the failure is corrected.



Note — Clearing the status also clears the associated alarm that is raised when post-discovery script execution fails.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens with the Discovery Rules tab displayed.

2 Click on the Managed State tab.

3 Click on the Search button. A list of NEs is displayed.

4 Select an NE with an Execution Status of Failed and click on the Properties button. The Node Discovery Control (Edit) form opens.

5 Click on the Post Discovery tab.

6 Click on the Clear button. The Script Execution Status changes from Failed to unspecified.

7 To execute the script, perform the following steps.

- **i** Click on the Execute Script button. The Execute script form opens.
- **ii** Click on the Execute button. The script executes, and a script object is displayed in the navigation tree of the form.
- **iii** Select the script object in the navigation tree.
- **iv** Expand the Status and Script Results panels on the right side of the form to reveal the script execution information.
- **v** Click on the Save Result button to save the result in the 5620 SAM database. A dialog box appears.
- **vi** Click on the OK button.
- **vii** Click on the Close button. The Execute script form closes.

8 Click on the OK button.

9 Close the Node Discovery Control form.

10 Close the Discovery Manager form.

Procedure 10-10 To configure an event notification policy

Perform this procedure to configure how the 5620 SAM processes specific SNMP traps from specific NE types and releases.



Caution — The 5620 SAM relies on certain SNMP notifications to verify network management activities. Before you configure an event notification policy, consult an Alcatel-Lucent support representative to ensure that you do not disable the processing of traps that are vital to 5620 SAM operation.

1 Choose Administration→Mediation from the 5620 SAM main menu. The Mediation (Edit) form opens.

2 Click on the Event Notification Policies tab.

3 Perform one of the following.

a Create a policy.

i Click on the Create button. The Event Notification Policy (Create) form opens.

ii Configure the parameters:

- Auto-Assign ID
- Policy ID
- Displayed Name
- Description
- Network Element Type

After the Network Element Type parameter is configured, the form expands to display the Product and Version panels.

iii Click on the Select button in the Version panel to choose the release of NE to which the policy is to apply. The Select Version - Event Notification Policy form opens with a list of available releases displayed.

iv Select a release and click on the OK button. The Select Version - Event Notification Policy form closes and the release information is displayed on the Event Notification Policy (Create) form.

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The Mediation (Edit) form reappears with the new policy in the list.

vii Click on the Apply button. A dialog box appears.

viii Click on the Yes button.

ix Select the new policy in the list and click on the Properties button. The Event Notification Policy (Edit) form opens.

b Modify a policy.

i Click on the Displayed Name column heading to sort the existing policies by device type and release.

ii Drag the Displayed Name column boundary to display the device type and release information.

iii Scroll through the list to locate the policy for the required device type and release using the information in the Displayed Name column.

iv Select the required policy and click on the Properties button. The Event Notification Policy (Edit) form opens.

v Configure the parameters:

- Displayed Name
- Description

4 Click on the Notification Policies tab. A list of SNMP traps is displayed.

5 Click on a column header, for example, MIB Name or MIB Entry Name, to sort the list alphabetically.

6 Select an SNMP trap entry in the list and click on the Properties button. The MIB Entry Policy - trappolicy (Edit) form opens.

7 Configure the Administrative State parameter.



Note — You cannot configure the Administrative State parameter in a default event notification policy. A default policy is indicated by a check mark beside the Default Policy indicator on the General tab of the Event Notification Policy (Edit) form.

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button. The MIB Entry Policy - trappolicy (Edit) form closes.

10 Repeat steps 6 to 9 to configure the processing of an additional SNMP trap by the 5620 SAM.

11 Close the Event Notification Policy (Edit) form.

12 Close the Mediation (Edit) form.

Procedure 10-11 To assign an event notification policy to an NE



Caution — The 5620 SAM relies on certain SNMP notifications to verify network management activities. Before you assign an event notification policy to an NE, consult an Alcatel-Lucent support representative to ensure that you do not disable the processing of traps that are vital to 5620 SAM operation.

1 Right-click on an NE icon in the navigation tree and choose Properties. The Network Element (Edit) form opens with the General tab displayed.

2 Click on the Polling tab.

3 Click on the Clear button in the Assigned Event Notification Policy panel. The Select button in the panel is enabled.

4 Click on the Select button in the Assigned Event Notification Policy panel to choose an event notification policy. The Select Event Notification Policy - Network Element form opens with a list of appropriate event notification policies for the device displayed.

5 Select a policy in the list and click on the OK button. The Select Event Notification Policy - Network Element form closes and the new policy identifier is displayed on the Network Element (Edit) form.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The Network Element (Edit) form closes and the policy is applied.

Procedure 10-12 To edit a discovery rule

Edit discovery rules when new devices are added to the network.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens.

2 Select a discovery rule from the list.

3 Click on the Properties button. The Topology Discovery Rule (Edit) form opens with the General tab displayed.

4 Configure the parameters, as required. For example, to remove a rule element:

- **i** Click on the Rule Elements tab.
- **ii** Select the rule from the list.
- **iii** Click on the Delete button.
- **iv** Confirm the action.

5 Click on the OK button to close the Topology Discovery Rule (Edit) form.

6 Perform steps 2 to 6 in Procedure 10-7.

7 Close the Discovery Manager form.

Procedure 10-13 To enable or disable a discovery rule

When a discovery rule is enabled, the network is scanned according to the discovery rule when the discovery rule is saved or rescanned. The network is also scanned according to the discovery rule as specified by the Discovery Rule Scan Interval parameter in the Mediation form. If your discovery rule is disabled, the network is not scanned as specified by these conditions.

1 Choose Administration→Discovery Manager from the main menu. The Discovery Manager form opens.

2 Select a discovery rule from the list.

3 Enable or disable the discovery rule.

   a Click on the Turn Up button to enable the discovery rule.

   b Click on the Shut Down button to disable the discovery rule.

Procedure 10-14 To delete a discovery rule

When you delete a discovery rule, only the rule is removed. The NEs discovered using the rule are not removed from the 5620 SAM, but the Discovery Rule ID for each of the NEs set to 0.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens.

2 Select a discovery rule in the list.

3 Click on the Delete button. A dialog box appears.

4 Click on the OK button.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Discovery Manager form closes.

Procedure 10-15 To rescan the network according to a discovery rule

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens.

2 Select one or more discovery rules from the list.

3 Click on the Rescan button.

4 Click Yes to confirm the action.

The 5620 SAM scans the network as specified by the discovery rules and discovers devices. After a device is discovered, the 5620 SAM server sets the device in a managed state and adds the NE properties to the 5620 SAM database.

5 Perform steps 3 and 6 in Procedure 10-7 to verify that the device has been successfully discovered.

Procedure 10-16 To manage, suspend, or unmanage a device

Perform this procedure to change the management state of a device.



Note — Managing and unmanaging a HIP device is not supported. To unmanage or delete a HIP device, you must set the EM system administrative state to Down, and then delete the EM system.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens.

2 Click on the Managed State tab.

3 Select a device in the list.

4 Perform one of the following.

a Click on the Manage button to return an unmanaged or suspended device to the managed state.

b Click on the Suspend button to suspend the management of the device.



Warning — Suspending the management of a device results in a loss of communication with the device.



Caution — When you suspend the management of a device, the 5620 SAM raises a critical alarm against the device.

c Click on the Unmanage button to stop the management of the device.



Warning 1 — Unmanaging a device results in a loss of management data for the device. See "Unmanaging and deleting devices" in section 10.1 for more information.

Warning 2 — Unmanaging a device results in the loss of all historical 5670 RAM AA statistics for the device.

A dialog box appears.

5 Click on the Yes button. The Managed State of the device changes to one of the following:

- managed, if you are remanaging the device
- suspended, if you are suspending management of the device
- not managed, if you are unmanaging the device

Procedure 10-17 To specify which management address the 5620 SAM uses to remanage a device

Perform this procedure to specify which management IP address is saved for a device when the device is set to an unmanaged state. You can configure the 5620 SAM to save the original management IP address or the most recently used management IP address for a device.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens.

2 Click on the Managed State tab.

3 Choose a device from the list.

4 Click on the Properties button. The Node Discovery Control (Edit) form opens with the General tab displayed.

5 Configure the Use Original Management IP parameter.

6 Click on the OK button. A dialog box appears.

7 Click Yes to confirm the action.

Procedure 10-18 To delete a device



Warning — Deleting a device results in a loss of management data and completely removes the device from the managed network. See section 10.1 for more information.

If you use the 5670 RAM to process 5620 SAM statistics, deleting an NE results in the loss of all historical 5670 RAM AA statistics for the device.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens.

2 Click on the Managed State tab.

3 Select a device in the list.

4 If the device is managed, click on the Unmanage button and wait for the state to change to Unmanaged. Otherwise, go to step 5.

5 Click on the Delete button. A dialog box appears.

6 Click on the Yes button. The device is deleted from the 5620 SAM database.

Procedure 10-19 To partially or fully resynchronize NEs with the 5620 SAM database

1 Perform one of the following.

a Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

b Open a physical or service tunnel topology map that displays the required NEs. See Chapter 6 for information about using topology maps.

2 Select one or more NEs, as required.

3 Choose a resynchonization option.

a Right-click on one of the selected devices you want to resynchronize with the 5620 SAM database and choose Resync→Resync All MIBs from the contextual menu.



Note — Choosing Resync All MIBs will fully resynchronize all MIBs for the devices, ignoring timestamps.

b Perform a partial resynchronization.

i Right-click on one of the selected devices you want to resynchronize with the 5620 SAM database and choose Resync→Customized Resync from the contextual menu. The Resync Site(s) form opens.

ii Select Choose MIB Entries.

iii Click on the Next button.

iv Select one or more MIB entries from the list.

v Click on the Next button.

vi Configure the Ignore Timestamps parameter.

vii Click on the Finish button and close the Resync Site(s) form.

4 Choose Administration→Discovery Manager from the 5620 SAM main menu.

5 Perform step 6 in Procedure 10-7 to verify that a particular device's properties have been added to the 5620 SAM database.

6 Close the Discovery Manager form.

Procedure 10-20 To list the active and mismatched SSH host keys

Perform this procedure to view the SSH2 host keys in order to identify the active and mismatched keys.

1 Open the SSH2 known host key manager by performing one of the following.

   a Choose Administration→Security→SSH2 Known Host Key from the 5620 SAM main menu.

   b Perform the following steps.

      i Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form appears.

      ii Click on the Managed State tab. A list of managed devices appears.

      iii Select a device in the list and click on the Properties button. The Node Discovery Control (Edit) form opens.

      iv Click on the Mediation Security tab.

      v Click on the SSH2 Known Host Key button. The SSH2 Known Host Key Manager form opens.

2 Configure the filter criteria and click on the Search button. A list of active and mismatched host keys appears.

3 Close the open forms, as required.

Procedure 10-21 To manually accept a mismatched SSH host key

Perform this procedure to manually accept a rejected SSH host key in order to establish a connection to the SSH server on an NE.



Caution — Before you accept a mismatched host key, you must verify the validity of the SSH connection.

1 Open the SSH2 Known Host Key Manager by performing one of the following.

   a Choose Administration→Security→SSH2 Known Host Key Manager from the 5620 SAM main menu.

   b Perform the following steps.

      i Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form appears.

      ii Click on the Managed State tab. A list of managed devices appears.

      iii Select a device in the list and click on the Properties button. The Node Discovery Control (Edit) form opens.

      iv Click on the Mediation Security tab.

      v Click on the SSH2 Known Host Key button. The SSH2 Known Host Key Manager filter form opens.

2 Choose Mismatch SSH2 Host Key as a match criterion using the drop-down list in the SSH2 Server Key Status column header.

3 Click on the Search button. A list of mismatched host keys is displayed.

4 Select the required host key entry.

5 Verify with the device administrator that the key fingerprint is the host key of the required device.

6 Click on the Delete button to delete the mismatched host key. The mismatched host key is deleted and a connection to the SSH server can be established.

7 Close the SSH2 Known Host Key Manager form.

8 Close open forms, as required.

Procedure 10-22 To change from SNMPv2c to SNMPv3 management of a device

1 Unmanage and delete the device.

   i Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form appears.

   ii On the Discovery Manager (Edit) form, select the device from the list that you want to manage using SNMPv3 and then click on the Unmanage button.

   iii When the device shows a Site State of Not Managed, click on the Delete button.

   iv Click OK on the Discovery Manager (Edit) form.

2 Perform Procedure 10-1 to create SNMPv3 groups and users on the device, and to create a discovery rule with an SNMPv3 mediation security policy.



Note — You can modify the existing discovery rule with an SNMPv3 mediation security policy. However, you must create a new discovery rule for the deleted device if not all devices discovered by the same rule are changed to SNMPv3 management.

3 Rediscover the device.

   i Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form appears.

   ii Click on the Discovery Rules tab.

   iii Select the discovery rule that was created in step 2 to discover the deleted device.

   iv Click on the Rescan button.

   v Click OK on the Discovery Manager (Edit) form.

Procedure 10-23 To switch from non-secure to secure mediation

1 Choose Administration→Mediation from the 5620 SAM main menu. The Mediation (Edit) form opens with the General tab displayed.

2 Click on the Mediation Security tab. You can create a mediation policy as described in Procedure 10-4, or modify the default mediation policy to use SSH2. Perform one of the following.

   a Click on the Create button to create a new mediation policy. The Mediation Policy (Create) form opens with the General tab displayed.

   b Choose the default policy from the list, and click on Edit. The Mediation Policy (Edit) form opens with the General tab displayed.

3 Configure the following parameters using the prescribed values:

- SSH2 as the Communication Protocol
- The SSH2 server user name and password as the User Name and User Password
- Secure as the File Transfer Type



Note — When the File Transfer Type is set to Secure, the Communication Protocol, User Name, and User Password parameters must be configured with the SSH2 information.

- The port that the NE uses for SSH2 communication as the SSH2 Server Port

4 Configure the remaining parameters on the form.

5 Click on the OK button. A dialog box appears.

6 Click on the OK button. The Mediation Policy form closes.

7 Click on the OK button. The Mediation (Edit) form closes.

8 Create a new discovery rule that uses the new SSH2 mediation policy as the read-access mediation policy and the write-access mediation policy. See Procedure 10-7 for information about creating discovery rules.

9 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form opens with the Discovery Rules tab displayed.

10 Click on the Managed State tab. A list of managed devices appears.

11 Choose the device from the list that you want to use SSH2 for CLI sessions and secure file transfers.

12 Click on the Properties button.

13 Click on the Mediation Security tab.

14 Choose the newly created SSH2 mediation policy as the read access mediation policy.



Note — You can also change the mediation policy for a discovery rule by performing step 14 and choosing a discovery rule from the Discovery Rules tab.

15 Click on the OK button. A dialog box appears.

16 Click on the Yes button. The Discovery Manager (Edit) form closes.

Procedure 10-24 To list and save SNMP MIB information

Perform this procedure to list and save SNMP MIB information, which may be of use for purposes such as the following:

- to maintain a record of the SNMP MIBs that the 5620 SAM supports
- to compare SNMP MIB support between 5620 SAM releases
- to identify the polling interval for a MIB entry

1 Choose Administration→Mediation from the 5620 SAM main menu. The Mediation (Edit) form opens with the General tab displayed.

2 Click on the MIB Entry Policies tab.

3 Configure the search filter and click on the OK button. The Mediation (Edit) form displays the MIB entry policies that match the search criteria.

4 To view the polling interval for a MIB entry, perform the following steps.

   i select the MIB entry and click on the Properties button. The MIB Entry Policy (Edit) form opens with the General tab displayed.

   ii View the polling interval setting in the Configuration panel.

   iii Close the MIB Entry Policy (Edit) form.

5 If required, sort the list according to the contents of a column by clicking on the column header.

6 If required, perform the following steps to save the listed information to a file.

   i Right-click on a column header and choose Save to File. the Save As form opens.

   ii Use the form to specify the file that is to contain the saved information.

   iii Click on the Save button. The information is saved to the specified file.

7 Close the Mediation (Edit) form.

11 — Device CLI sessions

11.1 Device CLI sessions overview *11-2*

11.2 Workflow to use a 5620 SAM CLI *11-3*

11.3 CLI procedures *11-3*

11.1 Device CLI sessions overview

You can perform most NE management functions using the 5620 SAM client GUI. Functions such as the following, however, require CLI access to a managed NE:

- validating GUI configuration actions
- configuring items that the GUI cannot, such as LI user access
- troubleshooting using device debug files

The 5620 SAM client GUI provides CLI access to the managed NEs from the main menu and from NE contextual menus in topology maps and navigation trees.



Note — When you use a CLI to change security parameters on an NE, the changes may not be synchronized with the 5620 SAM and subsequently not displayed in the GUI. For security reasons, the 5620 SAM cannot retrieve parameters such as passwords from an NE. To ensure that the security parameters are synchronized, you must use the client GUI to change the values.

Scope of command roles and user permissions on the cli package control CLI command access on an NE. The user permissions are set when security is configured on the NE locally or by using 5620 SAM configuration forms. See "NE user and device security" in the *5620 SAM System Administrator Guide* for information about setting NE access privileges.

vi editor support

On a 7450 ESS, 7710 SR, 7750 SR, or 7950 XRS, you can use the vi editor to modify local files. For example, after you use the 5620 SAM Scripts tool to create a CLI script, you can use a 5620 SAM CLI session to monitor the script execution on an NE, and then use the vi editor to modify the script. The vi editor is available in 5620 SAM Telnet and SSH sessions. The vi editor supports the standard vi navigation keys as well as the cursor keys (which are often called the arrow keys). See the appropriate device documentation for information about the supported vi commands and functions for a specific device.

See the appropriate device documentation for information about the device CLI command structure and usage. See "Script management" in the *5620 SAM Scripts and Templates Developer Guide* for more information about using the 5620 SAM Scripts tool to create CLI scripts.

11.2 Workflow to use a 5620 SAM CLI

The following workflow describes the sequence of high-level tasks required to open and use a device CLI from the 5620 SAM client GUI. The following must be true before you can use the 5620 SAM to open a device CLI using the GUI.

- The 5620 SAM user account has console access privileges on the managed devices. See "NE user and device security" in the *5620 SAM System Administrator Guide* for more information about user account privileges.
- The Telnet server on the managed devices is started.
- If required, SSH2 is properly configured on the managed devices; see chapter 10 for more information.

1 Configure the 5620 SAM CLI preferences. See Procedure 11-1 for more information.

2 Open a CLI session and log in to a managed device. See Procedure 11-2 for more information.

3 Configure the device, view device information, and modify files, as required.

4 Close the CLI session. See Procedure 11-1 for more information.

11.3 CLI procedures

The following procedures describe how to open CLI sessions using the 5620 SAM and configure the CLI console preferences.

Procedure 11-1 To configure the 5620 SAM CLI console preferences

Perform this procedure to customize the 5620 SAM CLI window settings. You can specify the following:

- the console text style and appearance
- the size of the scrolling buffer
- whether to save the session output to a file

1 Open a CLI session, as described in Procedure 11-2.

2 Right-click in the CLI window and choose Configure from the contextual menu. The Terminal Configuration form opens.

3 Configure the parameters:

- Minimum number of scrolling lines
- Font Name
- Font Size
- Bold
- Italic
- Foreground color
- Background color
- Send Console To a File
- Append to file
- Log File Location



Note — When the Send Console To a File parameter is enabled and the Append to file parameter is disabled, the log file is overwritten each time a new CLI session starts.

4 Click on the OK button. The Terminal Configuration form closes. The current and subsequent CLI sessions use the new settings.

Procedure 11-2 To open and close a 5620 SAM device CLI session

Perform this procedure to open a Telnet or SSH session on a managed device using the 5620 SAM client GUI.

1 Perform one of the following.

a Use the 5620 SAM navigation tree; perform the following steps.

i Choose Equipment from the view selector.

ii Right-click on a device icon.

iii Choose NE Sessions→*option* from the contextual menu

where *option* is Telnet Session or SSH Session

The Telnet Session or SSH Session window opens.



Note 1 — The managed device must be configured for Telnet access. See the appropriate device documentation for information about configuring Telnet access to the device.

Note 2 — SSH sessions use SSH2 by default on the 7210 SAS, 7450 ESS, 7750 SR, 7950 XRS, and GNEs. Ensure that SSH2 is properly configured on the device and that an SSH2 mediation policy is specified in the device discovery rule. See chapter 10 for more information about configuring SSH2 security.

b Use the 5620 SAM main menu; perform the following steps.

i Choose one of the following main menu options:

- Tools→Network Elements→NE Sessions→Telnet Session
- Tools→Network Elements→NE Sessions→SSH Session

The Telnet Session or SSH Session window opens.

ii Perform one of the following to specify an NE as the CLI session target.

- Type the management IP address of the NE beside the dimmed Connect button.
- Select an IP address from the drop-down menu.
- Click on the Select button to search for the NE.

The Connect button is enabled.

iii Click on the Connect button.

c Use the Manage Equipment form; perform the following steps.

i Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

ii Configure the filter criteria and click on the Search button.

iii Select an NE in the list.

iv Click on the NE Sessions button and choose Telnet Session or SSH Session. The Telnet Session or SSH Session window opens.

d Use a service topology map; perform the following steps.

i Choose one of the following from the 5620 SAM main menu:

- Manage→Service→Services
- Manage→Service→Composite Services
- Manage→Service→Mirror Services

The appropriate management list form opens.

ii Configure the filter criteria and click on the Search button.

iii Select a service in the list.

iv Click on the Topology View button. A dialog box appears.

v Click on the Yes button. A service topology map opens.

vi Right-click on an NE in the map and choose NE Sessions→Telnet Session or NE Sessions→SSH Session. The Telnet Session or SSH Session window opens.

e Use the Physical Topology map; perform the following steps.

i If the Physical Topology map is not open, choose Application→Physical Topology from the 5620 SAM main menu. The Physical Topology map opens.

ii Right-click on an NE in the map and choose NE Sessions→Telnet Session or NE Sessions→SSH Session. The Telnet Session or SSH Session window opens.

2 Enter the login credentials. You can use the CLI as specified by your user account permissions.

3 Perform NE management tasks, as required.

4 Click on the Disconnect button to close the CLI session.



Note — When you disconnect from a CLI session, the session window remains open to facilitate the opening of a subsequent CLI session.

5 Perform one of the following.

a Open a new CLI session; perform the following steps.

i Perform one of the following to specify an NE as the CLI session target.

- Type the management IP address of an NE beside the dimmed Connect button.
- Select an IP address from the drop-down menu.
- Click on the Select button to search for an NE.

The Connect button is enabled.

ii Click on the Connect button.

b Close the Telnet Session or SSH Session window.

12 — Working with network objects

12.1 Working with network objects overview *12-2*

12.2 Working with topology group objects *12-3*

12.3 Working with physical links *12-4*

12.4 Workflow to manage network objects *12-5*

12.5 Working with network objects procedures *12-5*

12.1 Working with network objects overview

The 5620 SAM is used to create, configure, and manage a device with the various children objects required to be part of a network. Equipment such as the routers, which are at the top of the hierarchy, have properties that are configured using the CLI and discovered when the 5620 SAM discovery process is run. After the device is discovered, it is displayed as an object in the navigation tree. See chapter 5 for more information about the navigation tree.

Objects in the 5620 SAM are considered to have parent/child relationships that are contained within a hierarchy. For example, a card in a card slot is the parent object of a daughter card. The behavior of each object is defined using parameters that are specific to the function required. Those parameters can be managed to suit the needs of the service required. Objects are created and managed using the properties forms found in the contextual menus of the equipment view.

The network is the top object in the navigation tree. The network icon in the navigation tree is the parent object of all managed devices. When you expand the network icon, all managed devices are shown as children of the network parent.

The device object is the discovered device at the top of the hierarchy in the navigation tree, directly below the network icon. The following children objects of the router are created automatically in the navigation tree after the device is discovered.

- CCAG
- ISA-Tunnel Group
- ISA-AA Group
- ISA-LNS Group
- ISA-NAT Group
- ISA-Video Group
- LAG
- IGH
- Shelf
- Card Slot
- Card Slot A for the CPM and switch fabric
- Card Slot B for the redundant CPM and switch fabric
- Fans
- Power Supplies
- CCM
- SFM Slot

The following objects must be created using property forms or create forms from the contextual menus of the equipment view or the ring group view.

- topology groups
- individual CCAGs with VSM-CCA members
- individual ISA-Tunnel Groups with ISA IPsec MDA members
- individual ISA-AA Groups with ISA-AA MDA members and ISA-AA partitions
- individual ISA-LNS Groups with ISA broadband applications MDA members
- individual ISA-NAT Groups with ISA broadband applications MDA members
- individual ISA-Video Groups with ISA-Video MDA members
- individual LAGs with subgroups of LAG member ports
- IGH members
- cards
- ring groups

- daughter cards
  Ports are automatically created when the daughter card is created.
- channels

Configuring an object is accomplished in two steps. First the object must exist or be created, second, the object parameters are modified. See Procedure 13-1 to create objects using the navigation tree.

Object deployment status

When you configure an object using the 5620 SAM GUI or the 5620 SAM OSS, the 5620 SAM saves the configuration and attempts to deploy the changes to the network. Although the value is changed on the configuration forms, the configuration change may not be fully deployed to the NE.

The 5620 SAM allows you to monitor the deployment state for objects. The Deployment tab on all object properties forms notifies you of configuration changes that are not fully deployed to the NE. The parameter that was unsuccessfully deployed is listed, along with the old value and the new value. A deployment icon or warning indicator appears in the following locations when you change the configuration of an object:

- beside all of the parameters on an object properties form for which a deployment is in progress (yellow icon) or has failed (red icon)
- beside the object in the navigation tree (blue icon, regardless of state)
- in info tables in map views (blue icon, regardless of state)
- in the Deployment column on object list forms (blue icon, regardless of state)
- on the Deployment tab (warning indicator)

See “NE maintenance” in the *5620 SAM System Administrator Guide* for information about how to configure a deployment policy, manage deployments, and troubleshoot failed deployments. See Procedure 12-1 for information about how to monitor the deployment of an object configuration change.

12.2 Working with topology group objects

The topology group icons in the navigation tree represent logical topology groups. Initially, a topology group object is created by choosing Create→Equipment→Group from the 5620 SAM main menu. A Group (Create) form opens. Additional topology groups can be created using the Copy button on the topology group properties form.

The Discovered NEs and the Unmanaged NEs topology groups are created by default. The Discovered NEs topology group contains the discovered devices. The Unmanaged NEs topology group contains unmanaged NEs that have been added to the network. You can create new topology groups and move devices to them using the topology maps.



Note — For existing topologies, the unmanaged NE will not be automatically moved to the Unmanaged NEs topology group in the following situations:

- existing unmanaged NEs
- managed NEs that are unmanaged

Although there is no limit to the number of topology groups, Alcatel-Lucent recommends a maximum of 10 000 topology groups per system for optimal performance. Each topology group can contain a maximum of 500 objects. Network elements and immediate child groups are considered objects in a topology group. A bracketed number is displayed beside the name of each topology group in the navigation tree. This number indicates the current number of objects in the group.

See chapter 6 for information about configuring topology group objects and managing topology groups using maps.

12.3 Working with physical links

The 5620 SAM allows you to create and manage links at the Layer 1 level. The physical links represent the actual physical configuration of network connections between ports. You can view and manage physical links from the physical topology map and the Manage Equipment list form.

Although there is no limit to the number of physical links you can have in a system, Alcatel-Lucent recommends a maximum of 10 000 physical links for optimal system performance.

Radio links between 9500 MPRs are shown as physical links by the 5620 SAM, with ports as the endpoint type.

See chapter 6 for information about configuring physical links and managing physical links using maps.

12.4 Workflow to manage network objects

The following workflow describes the sequence of high-level tasks required to manage and configure network objects. This workflow assumes that the physical devices have been installed, commissioned, and discovered. See chapter 9 for more information about device commissioning. See chapter 10 for more information about device discovery.



Note — Network objects can be accessed using the equipment navigation tree. See chapter 5 for more information.

1. As required, create network topology groups. See chapter 6 for more information.
2. As required, configure device objects. See chapter 13 for more information.
3. As required, configure logical group objects. See chapter 14 for more information.
4. As required, configure shelf, card, and daughter card objects. See chapter 15 for more information.
5. As required, configure port and channel objects. See chapter 16 for more information.
6. As required, create physical links. See chapter 6 for more information.
7. Monitor the deployment status of network objects. See Procedure 12-1 for information about how to monitor the deployment status of an object.

12.5 Working with network objects procedures

Use the following procedures to work with network objects.

Procedure 12-1 To monitor the deployment status of a network object

Perform the following procedure to monitor the deployment status of a configuration change to a network object. In addition, you can click on the Deployment tab if a warning indicator appears when you open a properties form

1. Open the properties form for the network object.
2. Configure the parameters, as required.
3. Click on the Apply button. An icon appears beside the modified parameter:
   - yellow icon—deployment in progress. The icon disappears when the deployment is successful.
   - red icon—failed deployment

   In addition, a blue deployment icon appears beside the NE object in the navigation tree, in list forms, and in configured info tables in map views.

A warning indicator appears on the Deployment tab.

4 Click on the Deployment tab.

5 Click on the Search button, if required.

6 In the Name column, verify the name of the parameter for which the deployment was unsuccessful. You can also verify the old value of the parameter before the change was applied, the new parameter value, and the deployer ID.

7 Navigate to the parameter on the configuration form that failed to deploy, if necessary, by selecting an entry in the Attributes list and clicking on the Show Attribute button. The attribute is higlighted for a few seconds on the configuration form.



Note — If you choose an entry in the Attributes list that is located on a hidden tab and click on the Show Attribute button, the hidden tab will temporarily be displayed. See Procedure 3-20 on how to configure hidden tabs.

8 Troubleshoot the cause of the failed deployment. See “To troubleshoot a failed configuration deployment” in the *5620 SAM System Administrator Guide* for more information. After you clear the deployer, all deployment icons disappear.

13 — Device object configuration

13.1 Device object configuration overview *13-2*

13.2 Working with device objects *13-2*

13.3 Working with ring group objects *13-2*

13.4 Workflow to manage device objects *13-3*

13.5 General device configuration procedures *13-5*

13.6 Ring group configuration procedures *13-24*

13.1 Device object configuration overview

The device object is the discovered device at the top of the hierarchy in the navigation tree, directly below the network icon.

This chapter contains the procedures to configure device objects using the navigation tree. Device object properties forms, which are used to configure specific parameters for discovered devices, are accessed using objects on the 5620 SAM navigation tree. See chapter 5 for more information about using the navigation tree.

13.2 Working with device objects

The device icons in the navigation tree represent device objects. Most of the configured properties for this object are inherited from the device. The Properties contextual menu option from the navigation tree allows you to configure or modify parameters for the object. These parameters are found on the respective tabs of the properties form and include the following:

- General
- Polling
- Protocols
- Load Balancing
- PAE Site
- Groups
- SAS Agent
- Faults

See chapter 9 for in-band and out-of-band management using parameters on the Polling tab. See chapter 8 for more information about the supported device types.

13.3 Working with ring group objects

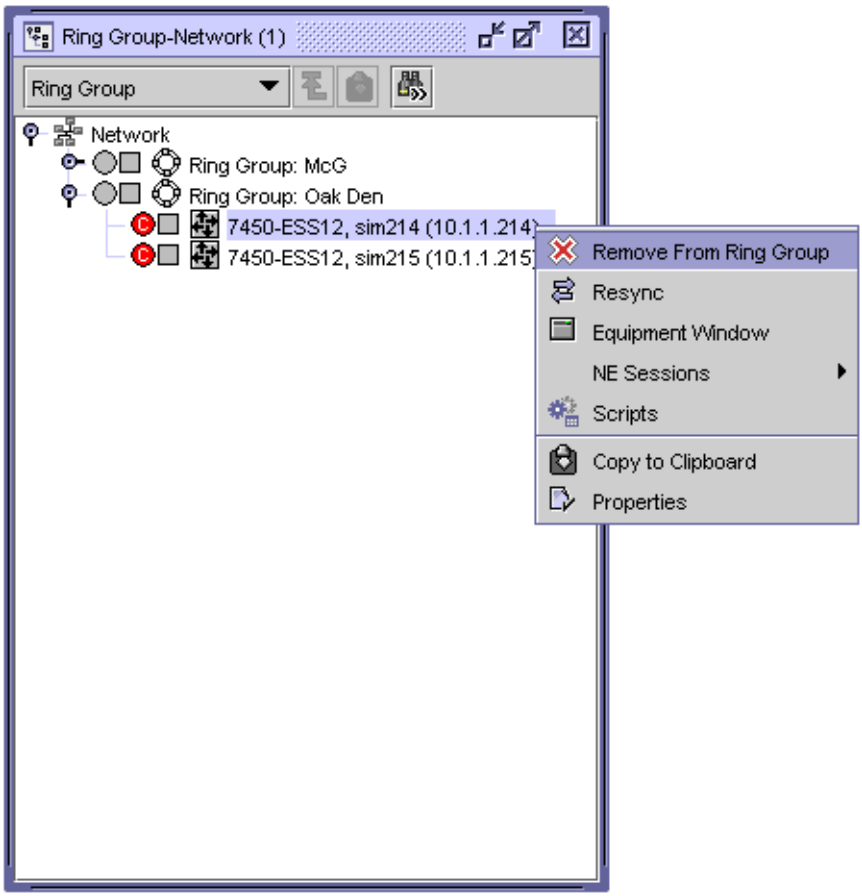
The 5620 SAM allows you to create and manage ring groups in the ring group view of the navigation tree. Ring groups are used to group devices logically to represent a typical network topology.



Note — The 5620 SAM uses VLAN groups instead of ring groups to group OmniSwitch NEs. See chapter 67 for more information about VLAN groups.

In the ring group view of the navigation tree, the network icon provides the contextual menu option Create Ring Group to create ring group icons. Using the properties form of a ring group, you can group devices logically in the ring group. Figure 13-1 shows a sample navigation tree ring group view.

Figure 13-1 Sample navigation tree ring group view



13.4 Workflow to manage device objects

The following workflow describes the sequence of high-level tasks required to manage and configure device objects. This workflow assumes that the physical devices have been installed, commissioned, and discovered. See chapter 9 for more information about device commissioning. See chapter 10 for more information about device discovery.

Note — Device objects can be accessed using the equipment navigation tree. See chapter 5 for more information about using the equipment navigation tree.

1 As required, configure the following general NE capabilities:

- **a** Create an object. See Procedure 13-1 for more information.
- **b** Modify an NE configuration. See Procedure 13-2 for more information.
- **c** Customize the NE property labels and values in the System preferences form, for example, to specify the location and site name that differs from the actual NE site name.

d Customize the NE property values in the NE form, see Procedure 13-3.

e Create an operational group. See Procedure 13-4 for more information.

f Enable and configure global cflowd on an NE, and create cflowd collectors. See Procedure 13-5 for more information.

g Associate a span of control with an NE. See Procedure 13-6 for more information.

h Configure 802.1x authentication on an NE. See Procedure 13-8 for more information.

i Configure active card alarms on an NE. See Procedure 13-10 for more information.

j Configure a TWAMP server. See Procedure 13-11 for more information.

k Enable LLDP on a router. See Procedure 13-12 for more information.

l Configure BFD flap detection on an NE. See Procedure 13-13 for more information.

m Create a chassis-level PBB configuration. See Procedure 13-15 for more information.

n Configure serving network information. See Procedure 13-16 for more information.

o Configure the RADIUS CoA port on an NE. See Procedure 13-17 for more information.

p Enable frame-based accounting on a 7210 SAS. See Procedure 13-19 for more information.

q Configure the system resource profile on a 7210 SAS. See Procedure 13-20 for more information.

r Configure the use of vendor-specific ICMP extensions on a 7705 SAR. See Procedure 13-21 for more information.

s Configure subscriber data persistence on the NE. See Procedure 13-22 for more information.

t Configure the QoS ingress aggregate rates on a 7705 SAR-M. See Procedure 13-23 for more information.

u Launch an MCT from a 9500 MPR NE connected to a 7705 SAR. See Procedure 13-24 for more information.

v Start and stop a Webview or Secure Webview session on an OmniSwitch. See Procedure 13-25 for more information.

w Configure the dying gasp alarm on an OS 6250 (Metro), OS 6850E, or OS 6855 NE. See Procedure 13-26 for more information.

2 As required, configure ring group objects. See Procedures 13-27 and 13-28 for more information.

13.5 General device configuration procedures

Use the following procedures to configure devices using the navigation tree.

Procedure 13-1 To create an object

1 Right-click on an empty object in the navigation tree to open the contextual menu.

2 Choose Properties or, when available, Create <*objectname*>.

The properties form or the create form, as applicable, opens.

3 Configure the parameters as required.

Certain object parameters are available for configuration. Configuring these parameters creates the object, however, after the object is created you may need to edit it using properties forms.

Procedure 13-2 To modify NE properties

1 Right-click on a discovered NE in the navigation tree and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

2 Use the form to view or modify the NE parameters, as required.

3 Click on the OK button to save the changes. A dialog box appears.

4 Click on the Yes button. The Network Element (Edit) form closes.

Procedure 13-3 To configure custom NE property values in the NE form

1 Choose Equipment or Routing from the navigation tree view selector. The navigation tree displays the Equipment or Routing view.

2 Right-click on the NE where you need to configure the values for the Custom NE Properties. The Network Element (Edit) properties form opens with the General tab displayed.

3 In the Custom Properties panel, configure the user-defined values.

4 Click on the OK button. A dialog box appears.

5 Click on the Yes button. The Network Element (Edit) properties form closes.



Note 1 — The NE custom properties support the extended character set including multi-byte characters.

Note 2 — The configured labels and values are displayed in the following locations. You can configure the labels and values, if required.

- NE list form: Choose Manage→Equipment→Equipment→Network Element (from the object drop-down menu). The appropriate columns display the values and labels.
- Tree labels: See Procedure 4-3.
- Topology labels: See Procedure 4-4.
- Info Table: See Procedure 6-14.
- Alarms: See Procedure 31-13.

Note 3 — You can also configure Custom NE property values using the 5620 SAM-O. See the *5620 SAM-O XML Reference*.

Note 4 — The 5620 SAM GUI supports localized language display. See chapter 3 for more information.

Procedure 13-4 To create an operational group

Multiple objects can be bundled in operational groups. If you change the status of the operational group, the status of every object in the group is changed.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on an *NE* icon and choose Properties. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Globals tab.

4 Click on the Service tab.

5 Click on the Operational Group tab.

6 Click on the Create... button. The Operational Group (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Group Name
- Hold Down Time
- Hold Up Time

8 Click on the OK button. A dialog box appears.

9 Click on the OK button. The Operational Group (Create) form closes and the Network Element form reappears with the new operational group in the list.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The Network Element form closes.

Procedure 13-5 To enable and configure global cflowd on an NE

Perform this procedure to enable global cflowd and configure cflowd parameters on an NE. You can also configure cflowd sampling for AA flows. See chapter 76 for information about configuring cflowd collectors for AA application groups.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on an NE and select Properties from the contextual menu. The NE properties form opens.

3 Click on the CFLOWD tab. The General tab is displayed.

4 Set the CFLOWD State parameter to Enabled. The form displays additional parameters.

5 Configure the remaining parameters:

- Active Time-out (minutes)
- In-Active Time-out (seconds)
- Cache Size
- Sample Rate
- Over Flow (percent)
- Administrative State
- Template Re-transmit (seconds)

6 Click on the Collector tab.

7 Perform the following steps to add a collector.

i Click on the Create button. The Cflowd Collector Configuration (Create) form opens.

ii Configure the parameters:

- Host Address
- Port Number
- Description
- Version
- Aggregation Type
- Autonomous System
- Template Type

The Aggregation Type parameter is configurable when the Version parameter is set to version-8.

The Autonomous System parameter is configurable when the Version parameter is set to version-5 or version-8.

The Template Type parameter is configurable when the Version parameter is set to version-9.

iii Click on the OK button. The Cflowd Collector Configuration (Create) form closes and a dialog box appears.

iv Click on the OK button. The collector is listed on the NE properties form.

8 Repeat step 7 to add another collector, if required.



Note — A global NE cflowd configuration can contain up to five collectors.

9 Click on the OK button. A dialog box appears.

10 Click on the Yes button. The NE properties form closes.

Procedure 13-6 To add a span of control to an NE

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on a discovered NE and choose Properties. The properties form for the NE opens.

3 Click on the Spans tab.

4 Click on the Add button. The Select Span(s) - Network Element form opens with a list of available spans.

5 Choose one or more spans to apply to the NE.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The Select Span(s) - Network Element form closes.

Procedure 13-7 To configure load balancing

1 Right-click on the managed NE for which you want to configure load balancing and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

2 Click on the Globals tab. The Load Balancing tab is displayed.

3 Configure the parameters:

- L4 Load Balancing
- LSR IP Load Balancing
- IP Load Balancing
- Multicast Enhanced Load Balancing
- Service ID Lag Hashing

To enable system-wide enhanced multicast load balancing to send multicast traffic over a LAG, set the Multicast Enhanced Load Balancing to true.

To improve the LAG spraying of VLL service packets when ECMP and LAG hashing are performed by the same NE, set the Service ID Lag Hashing parameter to true.

4 Click on the OK button. The Network Element (Edit) form closes.

Procedure 13-8 To enable or disable 802.1X



Note — Before you can create an 802.1X policy, 802.1X must be enabled on the NE. Before you can configure 802.1X on an Ethernet access port, 802.1X must be enabled on the NE and an 802.1X policy must be created and distributed to the NE.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the managed NE for which you want to enable or disable 802.1X and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Globals tab. The Load Balancing tab is displayed.

4 Click on the PAE tab.

5 Set the Administrative State parameter to Up.

6 Click on the OK button. The Network Element (Edit) form closes.

7 Repeat steps 2 to 6 for each NE for which you want to enable 802.1X.

To create and distribute 802.1X policies to the NEs that use 802.1X, see chapter 50.

To configure 802.1X on Ethernet access ports, see Procedure 16-1 in chapter 16.

8 To disable 802.1X on a managed NE, repeat steps 2 to 6 and set the Administrative State to Down.

Procedure 13-9 To configure exclusive policy editing on an NE

You can enable or disable an exclusive policy editing restriction on one or more NEs.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the managed NE for which you want to configure exclusive policy editing and select Properties.



Note — You can perform this procedure on multiple NEs if needed. Select the required NEs from the navigation tree, right-click on any one of them, and then select Properties.

The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Globals tab. The Load Balancing tab is displayed.

4 Click on the Exclusive Edit tab.

5 Perform one of the following:

a Configure the parameters:

- Timeout (Seconds)
- Use Exclusive Edit

Setting the Use Exclusive Edit for the selected NEs prevents their local policy definitions from being changed by global updates.

b Click on the Reset Exclusive Edit button. A confirmation message is displayed. Click on Yes.

This action is only available to admin and policy users and removes any exclusive edit locks that were previously set for the selected NE(s).



Note — The Reset Exclusive Edit option is also available in global routing policies under the Local Definitions tab.

6 Close the Network Element (Edit) form.

Procedure 13-10 To configure active card alarms on an NE

Use this procedure to configure a 7950 XRS, 7450 ESS, 7710 SR, or 7750 SR to view NE alarms through the CLI.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the NE where you want to configure active card alarms and select Properties. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Globals tab. The Load Balancing tab is displayed.

4 Click on the Alarm Management tab and configure the parameters:

- Alarm Management
- Maximum Cleared Alarms

5 Click on the OK button. The Network Element (Edit) form closes.

Procedure 13-11 To configure a TWAMP server

You can enable or disable Two-Way Active Measurement Protocol on a server and view session and connection statistics.



Note — You cannot configure a TWAMP server after an NE upgrade until the NE is fully resynchronized.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the managed NE for which you want to configure a TWAMP server and select Properties. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Globals tab. The Load Balancing tab is displayed.

4 Click on the OAM tab.

5 Scroll to the OAM TWAMP panel. The General tab is displayed.

6 Configure the Administrative Status parameter.



Note — To make changes to the following TWAMP server parameters, the Administrative Status parameter must be set to Disabled.

7 Expand the Server Configuration panel.

8 Configure the parameters:

- Inactivity Timeout (Seconds)
- Maximum Connections
- Maximum Sessions

9 If you are configuring a 7705 SAR, Release 6.0 R1 or later, the Reflector Configuration panel is displayed.

Expand the Reflector Configuration panel and configure the Reflector Test Session Timeout (Seconds) parameter.

10 Click on the Prefix tab.



Note — The objects listed in the table control the behavior of the TWAMP connections that match the defined IP prefix.

11 Perform one of the following:

a Click on the Create button to add a new prefix. The Prefix TWAMP Server (Create) form opens, with the General tab displayed.



Note — The 5620 SAM allows you to create an unlimited number of prefixes. However, an NE can only accept a maximum of 100 prefixes. If more than 100 prefixes are created in the 5620 SAM, the affected NE will issue a deployment error.

b Click on the Search button to display a list of existing prefixes. Select the required item from the list and click the Properties button. The Prefix TWAMP Server (Edit) form opens, with the General tab displayed.

12 Configure the parameters:

- Prefix Address
- Prefix Length
- Description
- Maximum # Connections
- Maximum # Sessions

13 Click on the Statistics tab.

14 Select either SrvConnStats (Assurance) or PrefixSrvStats (Assurance), as required, from the Select Object Type drop-down menu.

15 Select either Past 4 Hour(s) or No Filter, as required, from the filter selector.

16 Click on the Statistics Policies button and select Statistics Policy from the menu. The Statistics Policy form opens, with the General tab displayed.

17 Configure the parameters:

- Retention Time (hours)
- Administrative State
- Threshold Reporting State

18 Click on the Thresholds tab.

19 Perform one of the following, depending on your selection in step 14.

a Configure the PrefixSrvStats (Assurance) threshold parameters:

- Srv Pfx Conn Count Periodic Threshold
- Srv Pfx Conns Rejected Periodic Threshold
- Srv Pfx Session Count Periodic Threshold
- Srv Pfx Test Packets Rx Periodic Threshold
- Srv Pfx Test Packets Tx Periodic Threshold
- Srv Pfx Test Sess Abort Periodic Threshold
- Srv Pfx Test Sess Completed Periodic Threshold
- Srv Pfx Test Sess Rejected Periodic Threshold

b Configure the SrvConnStats (Assurance) threshold parameters:

- Conn Idle Time Periodic Threshold (seconds)
- Conn Session Count Periodic Threshold
- Conn Test Packets Rx Periodic Threshold
- Conn Test Packets Tx Periodic Threshold
- Conn Test Sess Completed Periodic Threshold
- Conn Test Sess Rejected Periodic Threshold

20 Click on the OK button. A dialog box is displayed.

21 Click on the Yes button. The Statistics Policy form closes.

22 Click on the OK button. The Prefix TWAMP Server (Create) form closes.

23 To view TWAMP statistics on a server:

i Perform steps 1 to 4 of this procedure.

ii Click on the Prefix tab.

iii Click on the Search button to display a list of existing prefixes. Select the required item from the list and click the Properties button. The Prefix TWAMP Server (Edit) form opens, with the General tab displayed.

iv Select either SrvConnStats (Assurance) or PrefixSrvStats (Assurance), as required, from the Select Object Type drop-down menu.

v Select either Past 4 Hour(s) or No Filter, as required, from the filter selector.

vi Click on the Collect or Collect All button. The system compiles the statistics and displays the available records in the table.

vii Select the required record from the table and click the Properties button. The Statistics Record is displayed.

viii Close the Statistics record form when your are finished.

ix Click on the OK button. The Prefix TWAMP Server (Create) form closes.

24 Close the Network Element (Edit) form.

Procedure 13-12 To enable LLDP on an NE

LLDP is a neighbor-discovery protocol that allows an NE to advertise its identity and capabilities to other NEs attached to the same physical IEEE 801 LAN. LLDP is a global NE function that you can configure from the 5620 SAM equipment navigation tree on NEs that use Ethernet connectivity. See section 22.1 for more information.

1 Choose Routing from the navigation tree view selector. The navigation tree displays the Routing view.

2 Navigate to the router object. The path is Network→*NE*.

3 Right-click the NE icon and choose Properties. The Network Element (Edit) form opens with the General tab displayed.

4 Enable LLDP by performing the following steps.

i Click on the Globals tab.

ii Click on the LLDP tab.

iii Configure the parameters:

- Administrative Status
- Transmission Interval (Seconds)
- Transmission Multiplier
- Re-Init Delay (Seconds)
- Maximum Consecutive Transmissions
- Fast Transmission Interval (Seconds)
- PDUs in Fast Transmission
- Notification Interval (Seconds)
- Transmission Delay (Seconds)
- Fast Start Repeat Count

The Administrative Status, Maximum Consecutive Transmissions, Fast Transmission Interval (Seconds), and PDUs in Fast Transmission parameters do not apply to the OmniSwitch.

The Transmission Delay (Seconds) and Fast Start Repeat Count parameters only apply to the OmniSwitch.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Network Element (Edit) form closes.

7 Enable LLDP on one or more ports, as required. See chapter 16 for information about configuring port objects.

Procedure 13-13 To configure the BFD flap detection interval on an NE

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on an NE and choose Properties. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Globals tab.

4 Click on the BFD tab.

5 Configure the Operational State Transition Interval parameter.

6 Click on the OK button. A dialog box opens.

7 Click on the Yes button. The Network Element (Edit) form closes.

Procedure 13-14 To configure an IP next hop limit on an NE

Complete this procedure to specify a global IP next hop limit for hosts' managed routes.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on an NE and choose Properties. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Globals tab.

4 Click on the Subscriber Management tab.

5 Configure the IP Next Hop Limit parameter.

6 Click on the OK button. A dialog box opens.

7 Click on the Yes button. The Network Element (Edit) form closes.

Procedure 13-15 To create a chassis-level PBB configuration

Perform this procedure to provide the PBB MAC name configuration at the NE level.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on an NE and choose Properties. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Globals tab.

4 Click on the Service tab and configure the parameters:

- PBB Source Backbone MAC Address
- MAC Notification Interval (seconds)
- MAC Notification Count

5 Click on the MAC Name tab and click on the Create button. The PBB MAC Name (Create) form opens with the General tab displayed. Configure the parameters:

- MAC Name
- MAC Address

6 Click on the OK button.

Procedure 13-16 To configure serving network information on an NE

Perform this procedure to configure serving network information on an NE.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on an NE and choose Properties. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Globals tab.

4 Click on the Serving Network tab and configure the parameters:

- Mobile Country Code
- Mobile Network Code

5 Click on the OK button.

Procedure 13-17 To configure the RADIUS CoA port on an NE

Perform this procedure to configure the RADIUS change of authorization port on an NE.



Note — You cannot configure the RADIUS CoA port on the 7950 XRS, Release 11.0 R1 or later.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on an NE and choose Properties. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Globals tab.

4 Click on the RADIUS tab.

5 Configure the RADIUS CoA Port parameter.



Note — If the routing instance is bound to a RADIUS proxy server and the RADIUS CoA port is set to 1812, all CoA messages are received by the RADIUS proxy server and dropped by port 1812.

6 Click on the OK button.

Procedure 13-18 To configure two WRED slopes on a 7210 SAS

The 7210 SAS-D and 7210 SAS-M support three WRED slopes per queue.

- High priority/in-profile TCP
- Low priority/out-of-profile TCP
- Non-TCP

Perform this procedure to specify whether only the high priority and low priority slopes are used, and non-TCP slopes are ignored. This configuration is supported on the 7210 SAS-D and 7210 SAS-M, Release 6.0 R1 or later.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the 7210 SAS NE for which you need to configure two WRED slopes and choose Properties. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the QoS tab.

4 Configure the Use WRED Slopes parameter.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Network Element (Edit) form closes.

Procedure 13-19 To enable frame-based accounting for QoS policies

Perform this procedure to enable frame-based accounting for QoS policies on 7210 SAS NEs.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the 7210 SAS NE for which you want to configure frame-based accounting and choose Properties. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Frame Based Accounting tab.

4 Configure the parameters:

- Egress
- Ingress

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Network Element (Edit) form closes.

Procedure 13-20 To configure the system resource profile on a 7210 SAS

Perform this procedure to allocate the system resources on a 7210 SAS. The functional areas for which you can allocate resources depend on the chassis type. Not all panels display for all devices. See "System resource profile" in section 8.5 and the NE documentation for more information about system resource allocation.



Note — System hardware resources are shared. Do not assign more than the available resources. Functions are disabled if you assign more than the amount of available resources.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the required 7210 SAS network element and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Globals tab.

4 Click on the System Resource Profile tab.

5 Configure the system resources in the Ingress Internal CAM Resources panel.

i Configure the G8032 Fast Flood (Configured) parameter.



Note — Configuration changes for the G8032 Fast Flood (Configured) parameter do not take effect until the NE is rebooted. The current state of the parameter is displayed in the G8032 Fast Flood (Active) field.

ii On the SAP Ingress Internal ACL panel, configure the parameters:

- Total ACL Resource
- MAC Resource
- IPv4 Resource
- 64-bit IPv4/v6 Resource
- 128-bit IPv4/v6 Resource
- 64-bit IPv6 Resource



Note 1 — The sum of the values for the MAC Resource, IPv4 Resource, 64-bit IPv4/v6 Resource, 128-bit IPv4/v6 Resource, and 64-bit IPv6 Resource parameters must not be greater than the value specified for the Total ACL Resource parameter.

Note 2 — 128-bit addresses consume two entries each of the available entry resources.

iii On the SAP Egress Internal ACL panel, configure the parameters:

- Total ACL Resource
- MAC Resource
- IPv4 Resource
- 128-bit IPv4/v6 Resource
- 64-bit IPv6 Resource



Note 1 — The sum of the values for the MAC Resource, IPv4 Resource, 128-bit IPv4/v6 Resource, and 64-bit IPv6 Resource parameters must not be greater than the value specified for the Total ACL Resource parameter.

Note 2 — 128-bit addresses consume two entries each of the available entry resources.

iv On the SAP Ingress QoS Resources panel, configure the parameters:

- Total QoS Resource
- MAC Resource
- IPv4 Resource
- IPv4/v6 Resource



Note — The sum of the values for the MAC Resource, IPv4 Resource, and IPv4/v6 Resource parameters must not be greater than the value specified for the Total QoS Resource parameter.

v On the Queues panel, configure the SAP Ingress Queues (Configured) parameter.



Note — Configuration changes for the SAP Ingress Queues (Configured) parameter do not take effect until the NE is rebooted. The current state of the parameter is displayed in the SAP Ingress Queues (Active) field.

vi On the Router panel, configure the Max ECMP Route Destinations (Configured) parameter.



Note — Configuration changes for the Max ECMP Route Destinations (Configured) parameter do not take effect until the NE is rebooted. The current state of the parameter is displayed in the Max ECMP Route Destinations (Active) field.

vii On the Ethernet CFM panel, configure the parameters:

- Total CFM Resource
- Up MEP Resource



Note — The value for the Up MEP Resource parameter must not be greater than the value for the Total CFM Resource parameter.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The Network Element (Edit) form closes.

Procedure 13-21 To enable or disable ICMP extensions

Use this procedure to configure the use of vendor-specific ICMP extensions on the 7950 XRS, 7450 ESS, 7705 SAR, 7710 SR, and 7750 SR NE types.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the NE where you want to configure ICMP extensions and select Properties. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the ICMP tab.

4 Configure the Vendor-Specific ICMP Extensions parameter.

5 Click on the OK button. The Network Element (Edit) form closes.

Procedure 13-22 To configure subscriber data persistence

Use this procedure to configure data persistence on an NE. The Node Persistence feature allows an NE to store dynamic object information in a file on the NE.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the NE where you want to configure data persistence and select Properties. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Node Persistence tab.

4 Configure the File Location and Description parameters on each of the following panels:

- ANCP
- Application Assurance
- DHCP Server
- NAT Port Forwarding
- Subscriber Management



Note — Configuring the File Location parameter for any of the above applications enables data persistency for that application. Ensure that the specified location has sufficient disk space to handle the volume of dynamic objects that will persisted on it.

5 Click on the OK button. The Network Element (Edit) form closes.

Procedure 13-23 To configure QoS ingress aggregate rates on the 7705 SAR-M/ME

Perform the following procedure to configure QoS access ingress and network ingress aggregate rates on the 7705 SAR-M/ME.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the 7705 SAR-M/ME on which you need to configure QoS ingress aggregate rates and choose Properties. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the QoS tab.

4 Configure the Aggregate Rate parameter in the Access Ingress panel and in the Network Ingress panel.

5 Click on the OK button. The Network Element (Edit) form closes.

Procedure 13-24 To launch an MCT on a 9500 MPRe NE connected to a 7705 SAR

The 5620 SAM supports an integrated MCT from the port or NE level on the 7705 SAR-8 and the 7705 SAR-18. The MCT is distributed with a NEtO client in the 5620 SAM. The MCT can be launched from the port that is associated with the MW link in the navigation tree or from the MW Link Member (Edit) form. You can configure radio parameters using the MCT.

Consider the following before you launch the MCT:

- Java version 1.6 is required to launch the MCT.
- The MCT is only supported on a Windows client; however, it is not supported on Windows 7.
- Only one MCT session can be open at a time.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on a discovered 7705 SAR-8 or 7705 SAR-18 NE and choose External Element Manager.

3 Choose the corresponding MW member from the list and click on the Launch MCT button.

4 Enter your login credentials and click on the OK button. A dialog box appears.



Note — If the client system does not have the required MCT packages, the packages are downloaded from the 5620 SAM and saved in a third-party folder.

5 Click on the Accept button. The MCT initialization starts, and the MCT main view screen appears.



Note — If the MCT is not installed on the client system, the MCT installer window opens. After the MCT is installed, the MCT main view screen appears for all subsequent launches, with the MCT version adjusted to the NE version from which the MCT launched.

Procedure 13-25 To start and stop a Webview or Secure Webview session on an OmniSwitch

Perform the following procedure to start and stop a Webview or Secure Webview session on an OmniSwitch.

1 To start a Webview or Secure Webview session:

- **i** Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.
- **ii** Right-click on a discovered OmniSwitch and choose Launch Webview or Launch Secure Webview. A web browser starts and the Webview or Secure Webview login screen appears.



Note — An alternative method of launching a Webview or Secure Webview session is to right-click on a discovered OmniSwitch in the Equipment view. Select Equipment Window from the contextual menu. The Equipment Window form opens. Select the Launch Webview or Launch Secure Webview button on the form.

- **iii** Enter your user name and password. After a successful login, the Chassis Management Home Page appears.

2 To stop a Webview or Secure Webview session:

- **i** Click on the Log Out text at the top of the Webview or Secure Webview window. A Confirm Log Out dialog box appears.
- **ii** Click on the Log Out button to end the Webview or Secure Webview session.

See the appropriate OmniSwitch *Switch Management Guide* for information about configuring and using Webview or Secure Webview.

Procedure 13-26 To configure the dying gasp alarm on an OS 6250M NE

Perform this procedure if you need to configure the dying gasp alarm on an OS 6250M, Release 6.6.3 or later. The dying gasp alarm is also applicable to the following NEs without any additional configuration:

- OS 6250SME (Metro), Release 6.6.3 or later
- OS 6450 (Metro), Release 6.6.3 or later
- OS 6850E, Release 6.4.5 or later
- OS 6855, Release 6.4.5 or later



Note — To view the dying gasp alarm on the 5620 SAM, the OS 6250M must be managed using SNMP v2 with the community string set to public.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on a OS 6250M icon and choose NE Sessions→Telnet Session. The Telnet Session window opens.

3 See step 5 of Procedure 9-2 to configure the NE to be managed using SNMP v2 with a community string configured to public.



Note 1 — If the Backup/Primary power supply fails, a major alarm will be raised. This alarm will be sent only to the first two SNMP stations configured on the NE. “Show snmp station” lists the management station address. SAM ip should be first or second.

Note 2 — The "Loopback 0" address should not be used for the source IP address field on the NE.

13.6 Ring group configuration procedures

Use the following procedures to manage ring groups using the navigation tree.

Procedure 13-27 To create a ring group

You can use the ring group creation function to:

- indicate a VLAN ring topology
- indicate a VPLS ring topology
- configure the properties of the ring group to provide VLAN Internet, BTV (MVR), and L2 VPN (TLS) services
- group devices by geographic region

Consider the following before you create a ring group.

- Ensure that the devices are commissioned, as described in chapter 9.
- Ensure that mediation policies are configured to allow CLI access to the managed devices, as described in chapter 10.
- If you want specific access interfaces to be part of a VLAN service, ensure that the parent device of the interface is a member of the ring group.

1 Choose Ring Group from the navigation tree view selector. The navigation tree displays the Ring Group view.

2 Right-click on the Network object and choose Create Ring Group. The Ring Group (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Group Name
- Description
- Ring Group Type

4 Click on the Apply button.

5 If you set the Ring Group Type parameter to VPLS in step 3, go to step 8.

6 Click on the TLS tab to configure L2 VPN parameters.

7 Configure the TLS parameters:

- Enabled
- Ethertype
- Jumbo Frame

The Ethertype and Jumbo Frame parameters are configurable when the Enabled parameter is selected.

8 Perform one of the following to add a device to the ring group.

a Perform the following steps to use the current properties form.

i Click on the Group Members tab.

ii Click on the Create button. The Select Network Elements form opens.

iii Choose one or more NEs and click on the OK button. A dialog box appears.

iv Click on the OK button. The Select Network Elements form closes and the selected devices are listed on the Ring Group (Create) form.

v Click on the OK button. A dialog box appears.

vi Click on the Yes button. The Ring Group (Edit) form closes and the device objects are listed in the navigation tree under the new ring group object.

b Perform the following steps to use the navigation tree.

i Right-click on the device object in the Equipment view of the navigation tree and choose Add To Ring Group from the contextual menu. The Select Group form opens to display a list of ring groups.

ii Choose the new ring group and click on the OK button. The Select Group form closes and the device object is listed under the ring group in the Ring Group view of the navigation tree.



Note — All device types can be added as members of a VLAN ring group. Only devices that support VPLS can be added to a VPLS ring group.

9 To apply a span of control to a ring group, click on the Spans tab.

i Click on the Add button. The Select Span(s) - Ring Groups form opens with a list of available spans.

ii Choose one or more spans of control to apply to the ring group.

iii Click on the OK button. The Select Span(s)-Ring Group form closes and a dialog box appears.

iv Click on the OK button.

10 Provision VLAN services, as described in chapter 66.

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The Ring Group (Create) form closes.

Procedure 13-28 To remove a ring group or ring group device

1 Choose Ring Group from the view selector in the navigation tree. The navigation tree displays the Ring Group view.

2 Navigate to the required ring group object. The path is Network→Ring Group.

3 To remove a device from the ring group, right-click on the device object under the ring group and choose Remove From Ring Group from the contextual menu. The device is removed from the ring group.

4 To remove a ring group:

i Perform step 3 for each device in the ring group to remove all devices from the ring group.

ii Right-click on the Ring Group object and choose Remove Ring Group from the contextual menu. A dialog box appears.

iii Click on the Yes button. The ring group is removed.



Caution — Removing a ring group deletes the VLAN services that are associated with the ring group.

14 — Logical group object configuration

14.1 Logical group object configuration overview *14-2*

14.2 Working with CCAG objects *14-2*

14.3 Working with ISA-AA groups *14-2*

14.4 Working with ISA-Tunnel groups *14-3*

14.5 Working with ISA-LNS groups *14-4*

14.6 Working with ISA-NAT groups *14-4*

14.7 Working with ISA-Video groups *14-4*

14.8 Working with ISA-WLAN GW groups *14-5*

14.9 Working with IGH objects *14-6*

14.10 Working with LAG objects *14-6*

14.11 Workflow to manage logical group objects *14-8*

14.12 Logical group object configuration procedures *14-9*

14.13 LAG configuration procedures *14-27*

14.1 Logical group object configuration overview

Logical group objects are children of the device object. They appear below the device object in the navigation tree. The following logical group objects are created automatically in the navigation tree after the device is discovered.

- CCAG
- ISA-AA Group
- ISA-Tunnel Group
- ISA-LNS Group
- ISA-NAT Group
- ISA-Video Group
- LAG
- IGH

Properties forms for logical group objects are accessed using the 5620 SAM navigation tree.

This chapter contains the procedures to configure logical group objects using the navigation tree. See chapter 5 for more information about using the navigation tree.

14.2 Working with CCAG objects

CCAGs are navigation tree objects located below device icons. CCAGs are configured manually using the CCAG object navigation tree menu and subsequent forms. For proper CCAG configuration, a VSM-CCA card must be present in the NE. In the navigation tree, a VSM-CCA card can be opened to show its ports. The ports are indicated by VSM Port x/y/z, which shows port type and the ID of the port.

You must configure the following in the CCAG configuration forms:

- General properties such as CCAG ID, Description, CCA Rate Enabled, CCA Rate, Access Adapt QoS, and Administrative State
- CCAG MDA Members which are compatible ports that can belong to a CCAG.

When you create a CCAG, the 5620 SAM creates virtual paths to be used as interconnections to bind services together. Two unidirectional paths are created: Alpha and Beta. For each path, three virtual ports are created: one for SAP-SAP connections, one for SAP-NET connections, and one for NET-SAP connections. The last two virtual ports are used to bind a service and a network interface together.

A maximum of eight cards can be added to a CCAG, with a maximum of eight CCAGs per NE.

14.3 Working with ISA-AA groups

ISA-AA groups provide AA load balancing, scaling, and redundancy on NEs that contain multiple ISA-AA MDAs. ISA-AA redundancy protects against card failure and minimizes service disruption during maintenance or protocol signature upgrades.

The 5620 SAM supports AA group configuration on the 7450 ESS, 7750 MG, and 7750 SR. An NE can have up to seven ISA-AA groups.



Note — A single-slot chassis does not support AA configuration.

ISA-AA group configuration requires the following:

- group number, which can be set only during group creation
- up to seven primary group members and one optional backup member
- one or more forwarding classes to divert to the AA group

You can use multiple ISA-AA groups to scale the application of AA policies, and can divide an AA group into partitions that are customized for specific VPN services. Each partition has an AA policy, and supports the configuration of custom protocols, applications, and application groups. Within a partition, you can use application service options, or ASOs, to create multiple application QoS policies, or AQPs. AA partitions support statistics collection and data reporting to the 5670 RAM.



Note — When you create an ISA-AA group or partition, a default AA policy is automatically created for the group or partition. When you delete a group or partition, the default policy is also deleted.

See chapter 76 for more information about AA groups, partitions, and policies. See Procedure 14-2 for information about creating ISA-AA groups and partitions. See Procedures 14-3 and 14-4 for information about configuring additional ISA-AA group and partition functions.

14.4 Working with ISA-Tunnel groups

ISA-tunnel groups provide redundancy for IPsec tunneling and encryption functions when multiple ISA-IPSEC MDAs are installed on an NE. ISA-IPSEC redundancy protects against card failure and minimizes service interruption during maintenance or protocol signature upgrades. You can configure up to four ISA-Tunnel groups on one NE.

An ISA-tunnel group can operate in one of the following modes:

- primary/backup active MDA
- multiple active MDAs

The primary/backup configuration provides fault tolerance in the event of an MDA failure. An ISA-tunnel group in a primary/backup configuration can contain a maximum of two MDAs.

Using multiple active MDAs provides load balancing in addition to fault tolerance. This mode of operation is supported on a 10.0 R4 or later 7750 SR in chassis mode D or higher, and on a 11.0 R1 or later 7450 ESS in mixed mode. You can include up to 16 MDAs in an ISA-tunnel group when the use of multiple active MDAs is enabled.

You can configure an ISA-tunnel group on a 7750 SR or 7450 ESS in mixed mode to act only as an IKEv2 responder during a MC IPsec switchover. This is the automatic behavior for dynamic tunnels, but not for static tunnels. See chapter 29 for more information about MC IPsec.

14.5 Working with ISA-LNS groups

The 5620 SAM supports the creation and configuration of ISA-LNS groups. ISA-LNS groups provide LNS PPP session termination on 7750 SR NEs. You can assign an ISA-LNS group to a tunnel group profile or a tunnel profile. When an operational L2TP tunnel is established, peers that are associated with the ISA-LNS group are automatically created. Session traffic is automatically balanced across the available active ISA broadband application MDAs in the group. You can add ISA broadband application MDAs to an ISA-LNS group, and up to four ISA-LNS groups on each NE. See Procedure 14-6 for information about how to create and configure an ISA-LNS group.

You must configure the following on the ISA-LNS groups configuration form:

- General properties, such as Group Number, Description, and Administrative State
- ISA-LNS Group members



Note — You can configure an ISA broadband application MDA only on an IOM3-XP module in a 7750 SR -7 or 7750 SR-12.

14.6 Working with ISA-NAT groups

An ISA-NAT group provides a redundant NAT function for routing instances using ISA Broadband Applications MDAs. See chapter 24 for information about ISA-NAT group configuration.

14.7 Working with ISA-Video groups

ISA-Video groups are created to provide packet buffering and packet processing in support of the IPTV video features.

When configured in the router, video ISAs are logically grouped into video groups. An ISA-Video group allows more than one video ISA to be treated as a single logical entity for a specific application, where the system performs a load-balancing function when it assigns tasks to a member of the group.

ISA-Video groups provide a redundancy mechanism to guard against hardware failure within a group. ISA-Video groups pool the processing capacity of all the group members and increase the application throughput because of the increased packet processing capability of the group.

You must configure the following on the ISA-Video groups configuration form:

- General parameters
- ISA-Video Group members

You can add up to four MDAs to an ISA-Video group, and up to four ISA-Video groups on each NE. All members of an ISA-Video group are primary members.



Note — If the parameter ad Insert server is enabled, only one MDA can be added to an ISA-Video group.

14.8 Working with ISA-WLAN GW groups

An ISA-WLAN GW group is used to represent multiple hardware adapters as a single entity, allowing for warm redundancy between multiple WLAN GW ISAs. Only one ISA-WLAN GW group can be created per NE. This group can be numbered 1 to 4, but this number must be exclusive and cannot be in use by an ISA-NAT group.

The ISA-IOM is the child of the ISA-WLAN GW group. Only an IOM3 with both ISA BB MDAs populated is valid for addition. A maximum of six IOMs can be added to an ISA-WLAN GW group, with a maximum active IOM limit of five per group. The required ISA-IOMs should be added before the ISA-WLAN GW group is turned administratively up.

ISA-WLAN GW members are created automatically by the NE when the ISA-WLAN GW group is administratively up, and deleted automatically when the administrative state is down. The number of members is equal to the active IOM limit.

You can globally list ISA-WLAN GW groups from the Manage→ ISA Functions→ ISA-WLAN main menu. ISA-WLAN GW groups can also be listed from Manage→ Equipment.

Soft GRE tunnels

Soft GRE tunnels are created dynamically by the NE when the first UE attempts to connect. The tunnel is used to backhaul traffic from the access point or residential gateway to the WLAN GW. The NE creates tunnels on a per-access point or per-residential gateway basis. Soft GRE tunnels terminate on the WLAN-GW ISA.

Soft GRE tunnels are viewable on the configuration form for base routing instances, VPRN routing instances, group interfaces, and ISA-WLAN GW groups. The Soft GRE Tunnels tab lists the soft GRE tunnels belonging to a given routing instance. User equipment information is viewable from the properties form for individual soft GRE tunnels. GTP session information (including bearer information) is viewable from the properties form for individual user equipment items. You can globally list Soft GRE tunnels from the Manage→ ISA Functions→ ISA-WLAN main menu.

14.9 Working with IGH objects

IGHs are navigation tree objects located below the device icon. IGHs are configured manually using the configuration forms available when you choose Create IGH from the IGH object navigation tree contextual menu.

You create an IGH to group together IP links and POS links so that if a configured number of links go out of service for any reason, the remaining links in the IGH go out of service too. This causes the routing protocols to re-converge to switch from the primary path to an alternate path.

The following requirements and restrictions apply to IGHs.

- IGHs are supported only on network links.
- IGHs are supported only on SONET/TDM interfaces with PPP auto encapsulation.
- A port or channel needs to be bound to a router interface after the member is added to an IGH.
- You can assign a port to only one IGH.

14.10 Working with LAG objects

LAGs are navigation tree objects located below a device icon which aggregate multiple network connections in parallel to increase throughput beyond what a single connection can sustain, and to provide redundancy in case one of the links fails.

LAGs are configured manually using the configuration forms available when you choose Create LAG from the LAG object navigation tree contextual menu.

The following minimum configuration is required to enable LACP.

- Enable LACP at either end of the LAG group.
- Set one end of the LAG group as LACP active.

You must configure the following in the LAG configuration forms:

- General properties, such as LAG description, configured address, encapsulation type, and administrative state
- Link aggregation group parameters, such as port threshold, port threshold action, and dynamic cost
- LACP parameters, such as LACP mode, LACP transmit interval, actor administration key, LACP transmission standby, and LACP selection criteria
- LAG members, which are the compatible ports that can belong to a LAG

Because all ports can have their own MAC address, when ports are part of a LAG, the LAG must have an MAC address.

The port configuration of the first port added to the LAG is used to compare with subsequently added ports. If a discrepancy is found with a newly added port, that port is not added to the LAG.

Up to 32 ports can be added to or removed from a LAG on XCM cards or IOM 3 and IMM cards in chassis mode D. Otherwise, up to only eight ports can be added to or removed from a LAG. All ports added to a LAG must have the same parameter settings.

Only ports belonging to one LAG subgroup are considered eligible members of a LAG and can be selected as active links.

See section 8.21 for OmniSwitch-specific LAG information.

See the *5620 SAM MPR User Guide* for 9500 MPR-specific LAG information.

LAG link mapping profiles

You can use a LAG link mapping profile to assign a specific LAG egress port to a SAP or interface, and control how egress traffic is handled if the specified port fails. You can then configure the specified port to perform admission control and QoS contract with the knowledge that all traffic for the SAP or interface will egress on that port. You can also specify a secondary port to handle traffic in the event that the primary port fails. See Procedure 14-14 for more information about creating LAG link mapping profiles.

LAG utilization TCAs

You can enable TCA on a LAG object and determine whether the LAG utilization value exceeds a TCA policy threshold. The following nodes support enabling TCA on LAG objects:

- 7710 SR
- 7450 ESS
- 7750 SR
- 7950 XRS
- 9500 MPR

You can associate a TCA policy with a LAG object from the TCA policy configuration form. See procedure 19-3 for information about applying an existing TCA policy to an object from the object properties form. The 5620 SAM compares the utilization value at each statistics collection to the threshold value in the TCA policy and raises an alarm when the LAG utilization value crosses the specified limit. You need to enable performance statistics collection on the LAG object to configure a TCA policy. See chapter 19 for more information about TCA.

L1 LAGs support collection of scheduled and on-demand statistics, and plotting of real-time and historical statistics. L2 and Ethernet LAGs support collection of scheduled statistics and plotting of historical statistics.

BFD on Ethernet LAGs

You can configure an Ethernet LAG to use BFD to speed up the detection of link failures. When BFD is enabled on a LAG, micro-BFD sessions are automatically created for each link in the group. The following nodes support enabling BFD on a LAG:

- 7450 ESS
- 7750 SR
- 7950 XRS

For information about configuring BFD on a LAG, see Procedure 14-15. For information about viewing micro-BFD sessions on a LAG, see Procedure 14-16.

14.11 Workflow to manage logical group objects

The following workflow describes the sequence of high-level tasks required to manage and configure logical group objects. This workflow assumes that the physical devices have been installed, commissioned, and discovered. See chapter 9 for more information about device commissioning. See chapter 10 for more information about device discovery.



Note — Logical group objects can be accessed using the equipment navigation tree. See chapter 5 for more information about using the equipment navigation tree.

1 As required, configure CCAG objects. See Procedure 14-1 for more information.

2 As required, create and configure ISA-AA groups and ISA-AA partitions. See Procedure 14-2 for more information. Additionally, perform the following, as required:

   a Add a subscriber policy override to an ISA-AA group or ISA-AA partition. See Procedure 14-3 for more information.

   b Enable and configure cflowd on an ISA-AA group or ISA-AA partition. See Procedure 14-4 for more information.

3 As required, configure ISA-Tunnel groups. See Procedure 14-5 for more information.

4 As required, configure ISA-LNS groups. See Procedure 14-6 for more information.

5 As required, create and configure ISA-NAT groups. See Procedure 24-1 for more information. Additionally, perform the following, as required:

   a Configure statistics on an ISA-NAT group. See Procedure 24-8 for more information.

   b Start or stop a NAT address-pool drain operation. See Procedure 24-10 for more information.

6 As required, configure ISA-Video groups. See Procedure 14-7 for more information.

7 As required, configure ISA-WLAN GW groups. See Procedure 14-8 for more information.

8 As required, configure IGH objects. See Procedure 14-9 for more information.

9 As required, configure LAG objects:

a Create and configure a LAG. See Procedures 14-10 and 14-11 for more information.

b Create and configure a LAG on an OmniSwitch. See Procedure 14-12 for more information.

c Create and configure a dynamic LAG member on an OmniSwitch. See Procedure 14-13 for more information.

d Create a LAG Link Mapping Profile. See Procedure 14-14 for more information.

e Configure BFD on a LAG. See Procedure 14-15 for more information.

14.12 Logical group object configuration procedures

Use the following procedures to configure NE logical groups using the navigation tree.

Procedure 14-1 To configure a CCAG

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the NE object in the equipment navigation tree.

3 Expand the Logical Groups objects in the equipment navigation tree.

4 Perform one of the following:

a To create a CCAG, right-click on the CCAGs object and choose Create CCAG. The CCAG (Create) form opens with the General tab displayed. Configure the CCAG ID parameter.

b To configure a CCAG, expand the CCAG object, right-click on the CCAG that you want to configure and choose Properties from the contextual menu. The CCAG (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Description
- CCA Rate Enabled
- CCA Rate (kbps)
- Access Adapt QoS
- Administrative State

6 Click on the CCAG MDA Members tab to view and add CCAG MDA members associated with this CCAG.

7 Click on the Create button. The CCAG MDA Member (Create) form opens.

8 Click on the Select button. The Select Member MDA - CCAG MDA Member form opens with a list of available VSM-CCA cards.

9 Choose the MDA to add to this CCAG and click the OK button. The Select Member MDA - CCAG MDA Member form closes and the CCAG MDA Member (Create) form reappears.

10 Click on the OK button. The CCAG MDA Member (Create) form closes.

11 Click on the CCAG Paths tab. The Alpha and Beta paths are displayed. To modify a path, go to step 12. Otherwise, go to step 25.

12 Choose a path and click on the Properties button. The CCAG Internal Path (Edit) form opens with the General tab displayed.

13 Configure the parameters:

- Path Rate Enabled
- Path Rate (Kb/s)
- Path Rate Option
- Path Weight (%)

14 Click on the Path Cross Connects tab. This tab displays the cross- connects associated with the path.

15 Choose a cross-connect to be configured and click Edit. The Cross Connect (Edit) form opens with the General tab displayed.

16 Configure the parameters:

- Description
- Configured MAC
- MTU (octets)

17 Click on the States tab.

18 Configure the Administrative State.

19 Click on the Policies tab.

20 To specify an egress slope policy other than the default, perform the following steps.

i Click on the Clear button in the Egress Slope Policy panel.

ii Click on the Select button in the Egress Slope Policy panel. The Select Egress Slope Policy form opens.

iii Choose a policy and click on the OK button. The Select Egress Slope Policy form closes and the policy name is displayed on the Cross Connect (Edit) form.

21 Configure the parameters:

- Committed Burst Size (%)
- Committed Burst Size (%)

22 To specify an ingress slope policy other than the default, perform the following steps.

i Click on the Clear button in the Ingress Slope Policy panel.

ii Click on the Select button in the Ingress Slope Policy panel. The Select Ingress Slope Policy form opens.

iii Choose a policy and click on the OK button. The Select Ingress Slope Policy form closes and the policy name is displayed on the Cross Connect (Edit) form.

23 Click on the OK button. The Cross Connect (Edit) form closes and the CCAG Internal Path (Edit) form reappears.

24 Click on the OK button. The CCAG Internal Path (Edit) form closes and the CCAG (Edit) form reappears.

25 Click on the OK button. The CCAG (Edit) form closes.

Procedure 14-2 To configure an ISA-AA group and ISA-AA partitions

Perform this procedure to create an ISA-AA group that contains one or more partitions. ISA-AA partitions provide ISA-AA group functions that are limited to the partition scope.



Note — When you create an ISA-AA group or partition, a default AA policy is automatically created for the group or partition. When you delete a group or partition, the default policy is also deleted.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the ISA-AA Groups object on an NE. The path is Network→NE→Logical Groups→ISA-AA Groups.



Note — You can also create or configure an ISA-AA group or partition by choosing Manage→ISA Functions→ISA-AA, and then using the list form that opens.

3 Perform one of the following.

a Create an ISA-AA group. Perform the following steps.

i Right-click on the ISA-AA Groups object and choose Create ISA-AA Group from the contextual menu. The ISA-AA Group (Create) form opens with the General tab displayed.

ii Configure the Group Number parameter.

iii Click on the Apply button. The form displays additional tabs and parameters, and the form name changes to ISA-AA Group (Edit).

b Configure an existing ISA-AA group. Perform the following steps.

i Expand the ISA-AA Groups object.

ii Right-click on the ISA-AA group that you want to configure and choose Properties from the contextual menu. The ISA-AA Group (Edit) form opens with the General tab displayed.

4 Configure the parameters:



Note — If you are configuring an existing AA group and the associated AA group policy has SAP dependencies, you cannot modify the Partitions parameter until you remove the SAP dependencies on the group policy.

- Description
- Operation Upon Failure
- Administrative State
- Partitions
- Subscriber Scale
- Overload Cut-Through
- Number of IPv4 Transit Prefix Entries
- Number of IPv6 Transit Prefix Entries
- Number of Remote IPv6 Transit Prefix Entries
- Maximum HTTP Enriched Packet Size (octets)
- Match All HTTP Requests
- HTTP X-Online-Host
- AA Subscriber Remote
- Tethering Detection Administrative State
- Capacity Cost High Threshold
- Capacity Cost Low Threshold
- Current OLC State
- Revert OLC State

The Maximum HTTP Enriched Packet Size (octets) parameter is configurable only on a 7750 MG:

The Tethering Detection Administrative State parameter is configurable only on a Release 5.0 or later 7750 MG.

The following parameters are configurable only on a 7750 SR:

- AA Subscriber Remote
- Number of IPv6 Transit Prefix Entries
- Number of Remote IPv6 Transit Prefix Entries

5 Perform the following steps to specify one or more ISA-AA MDAs for the ISA-AA group.

i Click on the ISA-AA Group Members tab.

ii Click on the Create button. The ISA-AA Group Member (Create) form opens.

iii Configure the ISA-AA MDA Role parameter.

iv Click on the Select button and choose an MDA from the Select Member MDA - ISA-AA Group Member form. The MDA slot number is listed on the ISA-AA Group Member (Create) form.

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The ISA-AA Group Member (Create) form closes and the MDA is listed on the ISA-AA Group Member (Create) form.



Note — After an NE reboot, the NE performs a rebalancing of the AA load. Because of this, the MDA slot number assigned to an AA subscriber or AA SAP on the AA Subscriber or AA SAP Summary form is displayed as Unassigned if the AA subscribers in the configuration file cannot be accommodated.

vii Perform steps 5 ii to vi to add another MDA, if required.

6 Perform the following steps to specify one or more traffic forwarding classes to divert to the ISA-AA group.

i Click on the ISA-AA Group Diverted FCs tab.

ii Click on the Create button. The ISA-AA Group Diverted FC (Create) form opens.

iii Configure the Forwarding Class Name parameter.

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The ISA-AA Group Diverted FC (Create) form closes.

vi Perform steps 6 ii to v to add another forwarding class, if required.

7 Perform the following steps to configure QoS for the group.

i Click on the QoS tab.

ii Click on the Egress From-Subscriber tab.

iii Configure the following parameters:



Note 1 — You must deselect the Default check box before you can use a slider to specify a Reserved CBS (%) or Buffer Utilization High Water Mark value.

Note 2 — The value of the Buffer Utilization High Water Mark parameter must be higher than the value of the Buffer Utilization Low Water Mark parameter.

- Reserved CBS (%)
- Buffer Utilization High Water Mark
- Buffer Utilization Low Water Mark

iv To specify a slope policy, click on the Select button in the Slope Policy panel and choose a slope policy from the Select Slope Policy form.

v To specify a network queue policy, click on the Select button in the Network Queue Policy panel and choose a policy from the Select Network Queue Policy form.

vi To specify a port scheduler policy, click on the Select button in the Port Scheduler Policy panel and choose a policy from the Select Port Scheduler Policy form.

vii Click on the Egress To-Subscriber tab.

viii Repeat steps 7 iii to vi.

8 If the Partitions parameter on the General tab is set to Enabled, perform the following steps to configure an AA partition for the group.



Note — If the Partitions parameter on the General tab is set to Enabled, the remaining procedure steps apply only to the partition; no more group configuration is required.

i Click on the ISA-AA Partitions tab.

ii To create a partition, perform the following steps.

- Click on the Create button. The ISA-AA Group Partition (Create) form opens with the General tab displayed.
- Configure the Partition ID parameter.
- Go to step 8 iv.

iii To configure an existing partition, select a partition in the list and click on the Properties button. The ISA-AA Group Partition (Edit) form opens with the General tab displayed.

iv Configure the parameters:

- Description
- Match All HTTP Requests
- HTTP X-Online-Host
- AA Subscriber Remote

9 To configure cflowd, perform Procedure 14-4.

10 To add one or more AA subscriber objects for statistics collection, perform the following steps.

i Click on the AA Subscriber Stats Objects tab.

ii Click on the Add button and choose one of the following options:

- Application
- Application Group
- Charging Group
- Custom Protocol
- System Protocol

The Select *object_type* form opens and lists the available objects of the chosen type.

iii Select an object in the list and click on the OK button. The elect *object_type* form closes and the AA Subscriber Stats Object Config form opens.

iv Configure the Export Method parameter.



Note — You can select both Export Method options only on a Release 11.0 or later 7750 SR.

v Click on the OK button. A dialog box appears.

vi Click on the OK button.

vii Repeat steps 10 ii to vi to add another statistics collection object, if required.

11 To add special-study objects to the ISA-AA group or partition, click on the AA Special Study tab. Otherwise, go to step 16.

12 To add a special-study subscriber to the group or partition, perform the following steps.

i Click on the Subscribers tab.

ii Click on the Create button. The AA Special Study Subscriber Config (Create) form opens.

iii Configure the parameters:

- AA Subscriber Name
- AA Stats Type

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The AA Special Study Subscriber (Create) form closes, and the subscriber is listed on the ISA-AA group or partition properties form.

13 To add one or more special-study SAPs to the ISA-AA group or partition, perform the following steps.

i Click on the SAPs tab.

ii Click on one or more of the following buttons and use the list form that opens to add one or more objects, as required:

- Add Per-SAP Protocols—to add a SAP for per-protocol monitoring
- Add Per-SAP Applications—to add a SAP for per-application monitoring

The list form closes, and the SAP is listed on the ISA-AA group or partition properties form.

14 To add one or more special-study spoke SDP bindings to the ISA-AA group or partition, perform the following steps.

i Click on the Spoke SDP Bindings tab.

ii Click on one or more of the following buttons and use the list form that opens to add one or more objects, as required:

- Add Per-Spoke SDP Binding Protocols—to add a SAP for per-protocol monitoring
- Add Per-Spoke SDP Binding Applications—to add a SAP for per-application monitoring

The list form closes, and the spoke SDP binding is listed on the ISA-AA group or partition properties form.

15 To add one or more special-study transit subscribers to the group or partition, perform the following steps.

i Click on the Transit Subscribers tab.

ii Click on the Create button. The AA Special Study Transit Subscriber Config (Create) form opens.

iii Configure the parameters:

- Transit Subscriber Name
- AA Stats Type

iv Click on the OK button. The AA Special Study Transit Subscriber Config (Create) form closes, and a dialog box appears.

v Click on the OK button. The transit subscriber is listed on the ISA-AA group or partition form.

16 To add an AA subscriber policy override to the ISA-AA group or partition, perform Procedure 14-3.

17 To configure one or more residential DCP groups, perform the following steps.

i Click on the 5670 RAM Parameters tab.

ii Click on the Create button. The Residential DCP Group (Create) form opens with the General tab displayed.

iii Configure the parameters:

- ID
- Auto-Assign ID
- Description
- Address Type
- Group Type

iv Click on the Address Rules tab.

v Click on the Create button. The DCP Address Rule (Create) form opens.

vi Configure the parameters:

- ID
- Auto-Assign ID
- Description
- IP Address Low
- High
- Mask

vii Click on the OK button. The DCP Address Rule (Create) form closes, and a dialog box appears.

viii Click on the OK button. The address rule is listed on the Residential DCP Group (Create) form.

ix Click on the OK button. The Residential DCP Group (Create) form closes, and a dialog box appears.

x Click on the OK button. The residential DCP group is listed on the ISA-AA group or partition properties form.

xi To create another residential DCP group, repeat steps 17 ii to x.

18 If you are configuring an ISA-AA partition, click on the OK button. The ISA-AA partition is listed on the ISA-AA group properties form.

19 Click on the OK button. A dialog box appears.

20 Click on the Yes button. The ISA-AA group properties form closes.

Procedure 14-3 To add an AA subscriber policy override to an ISA-AA group or partition

The AA subscriber policy override is rejected if the subscriber does not have an application profile assigned. You can add an AA subscriber policy override to a SAP or Spoke SDP, but not to an ESM subscriber.

1 If you are performing this procedure as part of the ISA-AA group or partition configuration described in Procedure 14-2, go to step 6.

2 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

3 Navigate to the ISA-AA group object. The path is Network→*NE*→Logical Groups→ISA-AA Groups→ISA-AA Group *n*.

4 Right-click on the ISA-AA Group *n* icon and choose Properties. The ISA-AA Group (Edit) form opens with the General tab displayed.

5 If you are configuring the subscriber policy override on an ISA-AA partition, perform the following steps.

i Click on the ISA-AA Partitions tab.

ii Select a partition in the list and click on the Properties button. The ISA-AA Group Partition (Edit) form opens.

6 Click on the AA Subscriber Policy Overrides tab.



Note 1 — An AA subscriber policy override is rejected if the subscriber does not have an assigned application profile.

Note 2 — You can add an AA subscriber policy override only for a SAP, spoke SDP binding, or transit subscriber.

7 Click on the Create button. The AA Subscriber Policy Override (Create) form opens with the General tab displayed.

8 Configure the AA Subscriber Type parameter.

9 Perform one of the following, based on the AA Subscriber Type parameter setting:

a If it is SAP, click on the Select button in the SAP Subscriber panel and choose a subscriber from the Select SAP Subscriber form.

b If it is Spoke SDP Binding, click on the Select button in the Spoke SDP Binding Subscriber panel and choose a subscriber from the Select Spoke SDP Binding Subscriber form.

c If it is Transit, click on the Select button in the Transit Subscriber panel and choose a subscriber from the Select Transit Subscriber form.

The subscriber is listed on the AA Subscriber Policy Override (Create) form.

10 Click on the ASO Characteristics tab.

11 Click on the Create button. The AA Subscriber Policy Override ASO Characteristic (Create) form opens.

12 Click on the Select button beside the Override ASO Characteristic Name parameter. The Select Application Service Option form opens.

13 Select an ASO in the list and click on the OK button. The ASO characteristic name is displayed on the AA Subscriber Policy Override ASO Characteristic form.

14 Click on the Select button beside the Override ASO Characteristic Value parameter. The Select Application Service Option Characteristic Value form opens.

15 Select an ASO Characteristic Value in the list and click on the OK button. The ASO characteristic value is displayed on the AA Subscriber Policy Override ASO Characteristic form.

16 Click on the OK button. The AA Subscriber Policy Override ASO Characteristic (Create) form closes, and a dialog box appears.

17 Click on the OK button. The AA subscriber policy override is listed on the ISA-AA group or partition properties form.

18 If you are configuring a partition, click on the OK button. The ISA-AA partition is listed on the ISA-AA group properties form.

19 Click on the OK button. A dialog box appears.

20 Click on the Yes button. The ISA-AA Group (Edit) form closes.

Procedure 14-4 To configure cflowd on an ISA-AA group or partition

Perform this procedure to enable or configure cflowd collectors on an ISA-AA group or partition.

1 If you are performing this procedure as part of the ISA-AA group or partition configuration described in Procedure 14-2, go to step 5.

2 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

3 Navigate to the ISA-AA group object. The path is Network→*NE*→Logical Groups→ISA-AA Groups→ISA-AA Group *n*.

4 Right-click on the ISA-AA Group *n* icon and choose Properties. The ISA-AA Group (Edit) form opens with the General tab displayed.

5 If you are configuring cflowd on an ISA-AA partition, go to step 16.

6 Click on the CFLOWD tab.

7 Configure the Sampling Rate parameter in the Volume panel.

8 Configure the parameters in the TCP Performance panel:

- Sample Flow Rate
- Sample Flow Rate 2

9 Configure the parameters in the RTP Performance panel:

- Sample Flow Rate
- Sample Flow Rate 2

10 Configure the parameters in the Comprehensive Performance panel:

- Comprehensive Flow Rate
- Comprehensive Flow Rate 2

11 Configure the remaining parameters:

- Template Re-transmit
- Administrative State

12 Click on the Collector tab.

13 Perform the following steps to add a collector.

i Click on the Create button. The Cflowd Collector (Create) form opens.

ii Configure the parameters:

- Host Address
- Collector Port
- Description
- Administrative State
- Version

iii Click on the OK button. The CFLOWD Collector (Create) form closes and a dialog box appears.

iv Click on the OK button. The collector is listed on the ISA-AA group properties form.

14 Repeat step 13 to add another collector, if required.



Note — An ISA-AA group can contain a maximum of two cflowd collectors.

15 Go to step 20.

16 Click on the ISA-AA Partitions tab.

17 Select a partition in the list and click on the Properties button. The ISA-AA Group Partition (Edit) form opens.

18 Click on the CFLOWD tab.

19 To add an AA application or application group for cflowd performance monitoring, click on the Performance tab. Otherwise, go to step 22.

20 To add an AA application for cflowd performance monitoring, perform the following steps.

i Click on the Add Applications RTP, Add Applications Comprehensive, or Add Applications TCP button. The Select Applications form opens.

ii Select one or more applications in the list and click on the OK button. The Select Applications form closes, and the applications are listed on the ISA-AA group or partition properties form.

21 To add an AA application group for cflowd performance monitoring, perform the following steps.

i Click on the Add Application Groups RTP, Add Application Groups Comprehensive, or Add Application Groups TCP button. The Select Application Groups form opens.

ii Choose one or more application groups in the list and click on the OK button. The Select Application Groups form closes, and the application groups are listed on the ISA-AA group or partition properties form.

22 To set the cflowd sampling administrative states, perform the following steps.

i Click on the States tab.

ii Configure the parameters:

- Volume Administrative State
- Performance Administrative State, in the following panels:
  - TCP Performance
  - RTP Performance
  - Comprehensive Performance

23 If you are configuring cflowd on an ISA-AA partition, click on the OK button to close the ISA-AA partition properties form. The ISA-AA group properties form reappears.

24 Click on the OK button. A dialog box appears.

25 Click on the Yes button. The ISA-AA group properties form closes.

Procedure 14-5 To configure an ISA-tunnel group

1 Choose Equipment from the network navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the NE object in the equipment navigation tree.

3 Expand the Logical Groups objects in the equipment navigation tree.

4 Perform one of the following:

a To create an ISA-tunnel group, right-click on the ISA-Tunnel Groups object and choose Create ISA-Tunnel Groups. The ISA-Tunnel Group (Create) form opens with the General tab displayed. Configure the Group Number parameter.

b To configure an ISA-tunnel group, expand the ISA-Tunnel Groups object, right-click on the ISA-tunnel group that you want to configure and choose Properties from the contextual menu. The ISA-Tunnel Groups (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Description
- Reassembly (msec)
- Administrative State
- Multiple Active ISA Support
- IPsec Responder Only
- Required Number of Active MDAs

6 Click on the Apply button.

7 Configure the parameters:

- Current OLC State
- Revert OLC State

8 Click on the ISA Tunnel Group Members tab.

9 Click on the Create button. The ISA Group Member (Create) form opens.

10 Click on the Select button. The Select Daughter Card - ISA Group Member form opens with a list of available ISA tunnel cards.

11 Choose the MDA to add to this ISA-Tunnel group and click the OK button. The Select Daughter Card - ISA Tunnel Group Member form closes and the ISA Group Member (Create) form reappears.

12 Click on the OK button. The ISA Group Member (Create) form closes.

13 Click on the OK button. A dialog box appears.

14 Click on the Yes button. The Tunnel Group form closes.

15 Repeat steps 9 to 14 to configure the backup ISA-Tunnel group member.

Procedure 14-6 To configure an ISA-LNS group

Perform this procedure to create and configure an ISA-LNS group. You can configure an IES or VPRN group interface to terminate LNS PPP sessions. See chapter 70 for information about configuring an IES group interface. See chapter 71 for information about configuring a VPRN group interface.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the NE object in the equipment navigation tree.

3 Expand the Logical Groups objects in the equipment navigation tree.

4 Perform one of the following:

a To create an ISA-LNS group, right-click on the ISA-LNS Groups object and choose Create ISA-LNS Groups. The ISA-LNS Group (Create) form opens with the General tab displayed. Configure the Group Number parameter.

b To configure an ISA-LNS group, expand the ISA-LNS Groups object, right-click on the ISA-LNS group that you want to configure and choose Properties from the contextual menu. The ISA-LNS Groups (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Description
- Administrative State
- Current OLC State
- Revert OLC State

The Current OLC State and Revert OLC State parameters are configurable when you click on the Apply button on the ISA-LNS Group (Create) form.

6 Click on the Select button in the Port Policy panel. The Select Port Policy form opens.

7 Choose a policy from the list and click on the OK button. The Select Port Policy form closes and your selection is displayed on the ISA-LNS Group (Create) form.

8 Click on the Apply button. The ISA-LNS Group (Edit) form opens with the General tab displayed.

9 Click on the ISA-LNS Group Members tab.

10 Click on the Create button. The ISA-LNS Group Member (Create) form opens with the General tab displayed.



Note — You can configure up to six ISA-LNS group members. For each group member, you must choose an ISA Broadband Applications MDA. An ISA Broadband Applications MDA can be configured only on an IOM3-XP module on a 7750 SR.

11 Click on the Select button. The Select Member MDA - ISA-LNS Group Member form opens with a list of available ISA broadband applications cards.

12 Choose the MDA to add to the ISA-LNS Group and click the OK button. The Select Member MDA - ISA-LNS Group Member form closes and the ISA-LNS Group Member (Create) form reappears. The Slot Name field displays your selection.

13 Click on the OK button. The ISA-LNS Group Member (Create) form closes.

14 Repeat steps 10 to 13 to configure another ISA-LNS Group member, if required.

15 Click on the OK button. A dialog box appears.

16 Click on the Yes button. The ISA-LNS Group Member (Create) form closes.

Procedure 14-7 To configure an ISA-Video group

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the NE object in the equipment navigation tree.

3 Expand the Logical Groups objects in the equipment navigation tree.

4 Perform one of the following:

a To create an ISA-video group, right-click on the ISA-Video Groups object and choose Create ISA-Video Groups. The ISA-Video Group (Create) form opens with the General tab displayed. Configure the Group Number parameter.

b To configure an ISA-video group, expand the ISA-Video Groups object, right-click on the ISA-Video group that you want to configure and choose Properties from the contextual menu. The ISA-Video Groups (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Description
- Administrative State
- Local Retransmission Server
- Fast Channel Change Server
- Ad Insert Server
- Reserve Retransmission Bandwidth (Mbps)
- Stream Selection
- Analyzer
- Current OLC State
- Revert OLC State

The Current OLC State and Revert OLC State parameters are configurable when you click on the Apply button on the ISA-Video Group (Create) form.

6 Click on the Apply button. The form displays four additional tabs.

7 Click on the Video Group Members tab.

8 Click on the Create button. The Video Group Member (Create) form opens.

9 Click on the Select button. The Select Daughter Card - Video Group Member form opens with a list of available ISA Video cards.

10 Choose the MDA to add to this Video Group and click the OK button. The Select Daughter Card - Video Group Member form closes and the Video Group Member (Create) form reappears. The Slot Name field displays your selection.

11 Click on the OK button. The Video Group Member (Create) form closes.

12 Repeat steps 5 to 11 to configure another ISA-Video Group member, if required.

13 Click on the OK button. A dialog box appears.

14 Click on the Yes button. The ISA-Video Group (Create) form closes.

Procedure 14-8 To configure an ISA-WLAN GW group

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the NE object in the equipment navigation tree.

3 Expand the Logical Groups objects in the equipment navigation tree.

4 Perform one of the following:

a To create an ISA-WLAN GW group, right-click on the ISA-WLAN GW Groups object and choose Create ISA-WLAN GW Groups. The ISA-WLAN GW Group (Create) form opens with the General tab displayed. Configure the Group Number parameter.

b To configure an ISA-WLAN GW group, expand the ISA-WLAN GW Groups object, right-click on the ISA-WLAN GW group that you want to configure and choose Properties from the contextual menu. The ISA-WLAN GW Groups (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Description
- Active IOM Limit

6 Click on the Select button beside the Port Policy parameter and choose a port policy from the Select Policy - ISA-WLAN GW Group form.

7 Click on the Select button beside the Tunnel Port Policy parameter and choose a port policy from the Select Port Policy - ISA-WLAN GW Group form.

8 Configure the parameters:

- Reservation Count
- Session Watermark High
- Session Watermark Low

9 Click on the Select button beside the NAT RADIUS Accounting Policy parameter and choose a NAT RADIUS accounting policy from the The Select Policy - ISA-WLAN GW Group form.

10 Click on the Apply button. The ISA-WLAN GW Group (Create) form refreshes with additional tabs, and the form name changes to ISA-WLAN GW Group (Edit).

11 Configure the parameters:

- Current OLC State
- Revert OLC State

12 Click on the ISA-IOMs tab.

13 Click on the Create button. The ISA-WLAN GW Group IOM (Create) form opens.

14 Click on the Select button. The Select Card form opens.

15 Select a card in the list and click on the OK button. The Select Card form closes and the ISA-WLAN GW Group (Create) form displays the card information.

16 Repeat steps 13 to 15 to configure another ISA-IOM, if required.

17 Click on the General tab.

18 Configure the Administrative State parameter.

19 Click on the OK button. A dialog box appears.

20 Click on the Yes button. The ISA-WLAN GW Group (Edit) form closes.

Procedure 14-9 To create an IGH and add members

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the IGHs object. The path is Network→*NE*→Logical Groups→IGHs.

3 Right-click on the IGHs icon and choose Create IGH. The Create IGH form opens with the Define General Properties step displayed.

4 Configure the parameters:

- IGH ID
- Minimum Active Link Threshold
- Administrative State

5 Click on the Next button. The Configure IGH Members step displays.

6 Click on the Create button. The Create IGH Member form opens with the Select Ports step displayed.

7 Configure the filter criteria, if required, and click on the Search button.

8 Choose a port from the list and click on the Finish button. The Create IGH Member form closes and a dialog opens.

9 Click on the OK button.

10 Repeat steps 6 and 9 to add more members, if required.

11 Click on the Finish button.

12 Click on the Close button. The Create IGH form closes.

14.13 LAG configuration procedures

Use the following procedures to manage LAGs using the navigation tree.

Procedure 14-10 To create a LAG

Note — This procedure applies to 7950 XRS, 7210 SAS, 7450 ESS, 7710 SR, 7705 SAR, and 7750 SR NEs. See Procedure 14-13 for information about how to configure a LAG on an OmniSwitch. See the *5620 SAM MPR User Guide* about how to configure a LAG on a 9500 MPR.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the NE object in the equipment navigation tree.

3 Expand the Logical Groups objects in the equipment navigation tree.

4 Right-click on the LAGs object and choose Create LAG from the contextual menu. The Create LAG step form opens.

5 Configure the parameters:



Note — The parameters that appear, and which can be configured, depend on the device type that the LAG is being configured for.

- Port Type
- Description
- Configured Address
- L2Uplink
- Mode
- Encapsulation Type
- Administrative State

If you are creating a LAG for HSMDA, the Port Type parameter must be set to hsmda. The Encapsulation Type must be either Dot1Q or QinQ. Setting Mode to network creates a network LAG, and setting it to access creates an access LAG.

If you are creating a LAG containing ports on an XMDA card on the 7705 SAR-18, then the Encapsulation Type must be either Dot1 Q or Null and the Mode must be set to Access.

6 If you are configuring a LAG on a 7210 SAS, you can add the LAG to an SHG. See Procedure 16-16 in chapter 16 for information about creating a 7210 SAS SHG.

i Click on the Select button in the Split Horizon Group panel. The Select Split Horizon Group - LAG form opens.

ii Choose an SHG and click on the OK button. The Select Split Horizon Group - LAG form closes and the Create LAG form refreshes with the SHG name.



Note 1 — A LAG cannot be added to or deleted from an SHG if it has a SAP configured on it.

Note 2 — A LAG cannot belong to more than one SHG; you must remove all SHGs from the LAG before you can add the LAG to a different SHG.

7 If you are configuring a LAG on a 7210 SAS-D 6F 4T ETR or 7210 SAS-E, go to step 12.

8 Click on the Next button. The Configure LAG Parameters form opens.

9 Configure the parameters:

- Port Threshold
- Port Threshold Action
- Dynamic Cost

10 Click on the Next button.

a If you set the Mode parameter in step 5 to Access or Hybrid, the Configure Access Parameters form opens. Go to step 11.

b If you set the Mode parameter in step 5 to Network, or if you did not configure the Mode parameter, the Configure LACP form opens. Go to step 13.

11 Configure the parameters:

- QoS Adaptation
- Enable Per Forwarding Path Ingress Queue
- Enable Per Forwarding Path Egress Queue
- Enable Lag Access Including Egress Hash Config



Note — If you are creating a LAG for HSMDA, the QoS Adaptation parameter must be set to Link, otherwise the LAG will not be created.

12 Click on the Next button. The Configure LACP form opens.

13 Configure the parameters:



Note — The availability of configurable parameters depends on the NE type for which the LAG is being configured.

- LACP Enabled
- Standby Signalling
- LACP Mode
- LACP Transmit Interval
- LACP Transmit Standby
- Auto-Generate
- Actor System ID
- Partner System ID
- LACP System ID
- LACP System Priority
- Actor System Priority
- Partner System Priority
- Hold Time (100s of milliseconds)
- Active Sub-Group Selection Criteria
- Slave to Partner

The LACP Mode, LACP Transmit Interval, Actor Administration Key, LACP System ID, and LACP System Priority parameters are configurable when the LACP Enabled parameter is enabled.

14 Click on the Next button. The Configure LAG Members form opens.

15 Click on the Create button to add network ports to LAGs. The Only show compatible ports form appears.

16 Configure the Show Only Compatible Ports and Class parameters.

17 Click on the Next button. The Select Ports form opens.

18 Choose compatible ports from the list to construct the LAG.

Add ports to the LAG as follows:

- Choose one or more ports. The maximum number of ports you can choose depends on the NE type.
- Click on the Next button. The Specify the Member Properties form opens.



Note 1 — For ports to appear as compatible ports, ensure no SAPs or services are configured on them.

Note 2 — You must use the same load balance algorithm for the ports associated with the LAG.

Note 3 — If there are no compatible ports to choose from and you want to edit some of the existing ports to be compatible, then disable the Show Only Compatible Ports parameter. Click on the Next button. Choose ports to edit from the list and click on the Properties button.

Note 4 — For HSMDAv2 ports in a LAG, you must set the Auto-negotiate parameter to False or Limited. Refer to Procedure 16-1 in chapter 16 for more information on configuring Ethernet ports.

Note 5 — If you are creating a LAG containing ports on an XMDA card in the 7705 SAR-18, then the following conditions apply to the ports:

- The Encapsulation Type must be set to either Dot1Q or Null.
- The Mode parameter must be set to Access.
- The Auto-negotiate parameter must be set to False or Limited.

19 Configure the parameters:

- Priority
- Sub-Group ID

20 If required, perform step 40 of Procedure 16-1 to add Egress Secondary Shapers to a port member of an HSMDA LAG. The following devices support this function:

- 7450 ESS-6
- 7450 ESS-7
- 7450 ESS-12
- 7750 SR-7
- 7750 SR-12



Note 1 — The add/delete/modify functions for Egress Secondary Shapers apply only to the primary port.

Note 2 — There can be a total of 64 egress secondary shapers per MDA, including the default shaper.

Note 3 — The Egress Secondary Shapers on the primary port of the LAG are propagated to each non-primary port member of the LAG, with a maximum 8 ports per LAG. These propagated shapers cannot be deleted.

For adding any new port to the LAG, the user must configure each Egress Secondary Shaper as per the primary port, otherwise the addition of the port is blocked.

Note 4 — When adding a port member to a LAG, the primary port and each selected port (maximum 8 ports) secondary shapers must have the same name and rate.

Ports with Egress Secondary Shapers cannot be added to a configured LAG which do not match the Egress Secondary Shapers of the primary port.

Note 5 — Shapers are not removed from the port when the port is removed from a LAG.

Note 6 — The SAP reference to the Egress Secondary Shapers within a LAG is supported. Only the primary port of the SAP on the LAG is used to determine the list of Egress Secondary Shapers for the SAP.

When port members are removed from the LAG, care must be taken to ensure that the last port member is not removed if the LAG is referenced to a SAP. Shapers must exist on a LAG to be referenced on a SAP. See chapters 61 to 74 for more information.

21 Click on the Finish button. The Specify Member Properties form closes and the Configure LAG Members form reappears. A dialog box appears.

22 Click on the OK button.

23 Click on the Finish button. The Configure LAG Members form closes and the Create LAG form reappears.

24 Click on the Close button.

25 Use the Properties contextual menu to view information about the created LAG or to modify LAG parameters.

- The General tab displays the LAG ID, the LAG description and configured MAC address.
- The Link Aggregation Group tab displays the threshold parameters, cost information, and the primary port in the LAG, along with all the other LAG member ports.
- LAG member ports can be added from the LAG Members tab.
- Statistics, terminations, and fault information is available from the appropriate tabs.

26 Expand the LAG object in the navigation tree to view the created LAG groups. Expand the LAG group object to view the subgroup member ports, the priority, the subgroup ID, and the subgroup mode.

Procedure 14-11 To configure a LAG



Note — This procedure applies to 7950 XRS, 7210 SAS, 7450 ESS, 7710 SR, 7705 SAR, and 7750 SR NEs. See Procedure 14-13 for information about how to configure a LAG on an OmniSwitch. See the *5620 SAM MPR User Guide* for information about how to configure a LAG on a 9500 MPR.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the LAG object that you want to configure. The path is Network→*NE*→Logical Groups→LAGs→LAG *n*.

3 Right-click on the LAG *n* icon and choose Properties. The LAG (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- Description
- Configured Address
- Mode
- Current OLC State

5 If you are configuring a LAG on a 7210 SAS you can add the LAG to an SHG. See Procedure 16-16 in chapter 16 for information about creating a 7210 SAS SHG.

i Click on the Select button in the Split Horizon Group panel. The Select Split Horizon Group - LAG form opens.

ii Choose an SHG and click on the OK button. The Select Split Horizon Group - LAG form closes and the Create LAG form refreshes with the SHG name.



Note 1 — A LAG cannot be added to or deleted from an SHG if it has a SAP configured on it.

Note 2 — A LAG cannot belong to more than one SHG; you must remove all SHGs from the LAG before you can add the LAG to a different SHG.

6 If you are configuring a LAG on a 7210 SAS, go to step 11.

7 Click on the Link Aggregation Group tab.

8 Configure the parameters:

- Port Threshold
- Port Threshold Action
- Dynamic Cost

9 Click on the States tab.

10 Configure the Administrative State parameter.

11 Click on the Access tab.

12 Configure the parameters:

- QoS Adaptation
- Enable Per Forwarding Path Ingress Queue
- Enable Per Forwarding Path Egress Queue
- Enable Lag Access Including Egress Hash Config



Note — If you are configuring a LAG for HSMDA, the QoS Adaptation parameter must be set to Link.

13 Click on the LACP tab.

14 Configure the parameters:

- LACP Enabled
- LACP Mode
- LACP Transmit Interval
- LACP Transmit Standby
- Auto-Generate
- Actor System ID
- Partner System ID
- LACP System ID
- LACP System Priority
- Actor System Priority
- Partner System Priority
- Hold Time (100s of milliseconds)
- Active Sub-Group Selection Criteria
- Slave to Partner

The LACP Mode, LACP Transmit Interval, and Actor Administration Key parameters are configurable when the LACP Enabled parameter is enabled.

15 Click on the Next button. The Configure LAG Members form opens.

16 Click on the LAG Members tab. To add LAG members, perform steps 15 to 23 of Procedure 14-10.

17 If the LAG that you are configuring is in Network mode, the Network Interfaces tab is displayed. Click on the Create button. The Create Network Interface form opens. Perform steps 4 to 50 of Procedure 22-9 to create a network interface. Otherwise go to step 21.

18 If the LAG that you are configuring is in access mode or hybrid mode with dot1q or QinQ encapsulation, or in network mode with dot1q encapsulation, the MEPs tab is displayed. To add a facility MEP to the LAG:



Note — Only one facility MEP can be configured on a LAG.

i Click on the MEPs tab.

ii Click on the Create button. The MEP (Create) form opens on the General tab.

iii Click on the Select button to choose a global MEG. The Select Maintenance Entity Group form opens.

iv Choose an entry and click on the OK button. The Select Maintenance Entity Group form closes.

v Configure the parameters:

- Auto-Assign ID
- Description
- CCM Messages Enabled
- Interface Type
- Priority Level for CCM Messages
- CCM TLV Ignore
- Low-priority Defect
- MAC Address
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)
- CCM Padding Packet Size (Bytes)
- Facility Fault Notify
- Facility VLAN ID



Note 1 — To enable fault propagation on a LAG facility MEP, Facility Fault Notify must be enabled.

Note 2 — The CCM Padding Packet Size (Bytes) parameter cannot be configured when the CCM interval parameter is set to 10 ms or 100 ms.

vi If the MD for the MEP has a Name Type of none the Y.1731 Tests tab is configurable; click on the Y.1731 Tests tab. Otherwise, go to step vii.

vii Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

viii Click on the OK button. A dialog box appears.

ix Click on the OK button. The MEP (Create) form closes.

19 To add a tunnel facility MEP to the LAG, perform the following steps.



Note — The LAG that you are configuring must be in Access mode or Hybrid mode and must have an encapsulation type of QinQ.

i Click on the MEPs tab.

ii Click on the Create button. The MEP (Create) form opens on the General tab.

iii Click on the Select button to choose a global MEG. The Select Maintenance Entity Group form opens.

iv Choose an entry and click on the OK button. The Select Maintenance Entity Group form closes.

v Configure the parameters:

- Auto-Assign ID
- Description
- CCM Messages Enabled
- Interface Type
- Priority Level for CCM Messages
- CCM TLV Ignore
- Low-priority Defect
- MAC Address
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)
- CCM Padding Packet Size (Bytes)
- Facility Fault Notify
- Facility VLAN ID



Note 1 — To enable the fault propagation on a tunnel facility MEP, Facility Fault Notify must be enabled.

Note 2 — To link the tunnel facility status to the SAP, Facility VLAN ID must match the outer encapsulation value of the SAP.

Note 3 — To accept the fault notification from a facility MEP on the site where the SAP is located and on the SAP, Tunnel Fault Management must be set to Accept.

Note 4 — The CCM Padding Packet Size (Bytes) parameter cannot be configured when the CCM interval parameter is set to 10 ms or 100 ms.

vi If the MD for the MEP has a Name Type of none the Y.1731 Tests tab is configurable; click on the Y.1731 Tests tab. Otherwise, go to step vii.

vii Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

viii Click on the OK button. A dialog box appears.

ix Click on the OK button. The MEP (Create) form closes.

20 To configure Ethernet-CFM redundancy on a facility MEP:



Note 1 — You must enable Ethernet CFM redundancy globally on a device before it can function on child objects such as LAGs. See chapter 13 for information about device object configuration.

Note 2 — The tunnel MEP must be part of an MC-LAG with Ethernet CFM redundancy configured.

i Click on the MEPs tab.

ii Click on the Search button. A list of MEPs is displayed.

iii Choose the facility MEP for which you need to configure Ethernet-CFM redundancy and click on the Properties button. The MEP (Edit) form opens.

iv Scroll to the Facility MEPS panel and select the Create Redundant MEP check box.

v Click on the OK button. The MEP (Edit) form closes. A redundant tunnel MEP with the same ID and Operational MAC address is created on the peer LAG. The redundant MEP has the same state as the MC-LAG in which that MEP resides.

21 Click on the OK button. A dialog box appears.

22 Click on the Yes button. The LAG (Edit) form closes.

Procedure 14-12 To configure an OmniSwitch LAG

Perform the following procedure to configure a static or dynamic LAG.

Workflow for a static LAG:

- create a static LAG on the local and remote switches
- assign ports to the LAG on the local and remote switches
- create a VLAN for the static LAG on the local and remote switches (optional)

Workflow for a dynamic LAG:

- create a dynamic LAG on the local (actor) and remote (partner) switches
- assign ports with the same actor administrative key (which allows them to be aggregated) to the local and remote LAG
- create a VLAN for the dynamic link aggregation group on the local and remote switch (optional)



Note 1 — You can configure MVRP fixed ports/LAGs, 802.1 Q ports/LAGs, aggregate ports/LAGs, and VLAN Stacking Network ports/LAGs.

Note 2 — When a port is assigned to a LAG member, you cannot modify the port properties using the 5620 SAM.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure the LAG and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Logical Groups icon.

4 Expand the LAGs icon, right-click on a LAG object and choose Create LAG from the contextual menu. The Create LAG - Define General Properties form opens.

5 Configure the parameters:

- LAG ID
- Auto-Assign ID
- Mode
- Administrative State
- Automatic VLAN Binding

The Automatic VLAN Binding parameter can only be configured for network LAGs and Stacked VLANs.

6 Click on the Next button. The Create LAG - Configure LAG Parameters form opens.

7 Configure the parameters:

- Size
- Name
- Type

8 Perform one of the following:

a If you set the Type parameter to Static, go to step 15.

b If you set the Type parameter to Dynamic, go to step 9.

9 Click on the Next button. The Create LAG - Configure LACP form opens.

10 Configure the parameters:

- Actor Administration Key
- Actor System ID
- Partner System ID
- Actor System Priority
- Partner System Priority
- Partner Administration Key

11 Click on the Finish button. The Create LAG - Wizard Completed form opens.

12 Enable the View the newly created interface check box if you need to view the LAG properties.

13 Click on the Close button. The Create LAG form closes.

See Procedure 14-13 in this section for information about adding members to a dynamic LAG.

14 Go to step 25.

15 Click on the Next button. The Create LAG - Configure LAG Members form opens.

16 Click on the Create button to add ports to the LAG. The Create LAG Member - Only show compatible ports form appears.

17 Configure the Show Only Compatible Ports and Class parameters.

18 Click on the Next button. The Create LAG Member - Select Ports form opens.

19 Click on the Search button to display a list of compatible ports. Choose ports from the list to construct the LAG.

Add ports to the LAG as follows:

- Choose up to the maximum number of ports you require from the list of ports. You can select more than one port at a time from the list.
- Click on the Next button. The Specify the Member Properties form opens.



Note 1 — If there are no compatible ports to choose from and you want to edit some of the existing ports to be compatible, then disable the Show Only Compatible Ports parameter. Click on the Next button. Choose ports to edit from the list and click on the Properties button.

Note 2 — Mobile, UNI, and NNI ports cannot be members of a LAG.

Note 3 — Only network ports can be members of a network LAG and only access ports can be members of an access LAG.

20 Click on the Finish button. A dialog box appears.

21 Click on the OK button. The Create LAG - Configure LAG Members form displays the LAG members.

22 Click on the Finish button. The Create LAG - Wizard Completed form opens.

23 Enable the View the newly created interface check box if you need to view the LAG properties.

24 Click on the Close button to close the form.

25 Use the Properties contextual menu to view information about the created LAG or to modify LAG parameters.

- The General tab displays the LAG ID and LAG description.
- The Link Aggregation Group tab displays the primary port in the LAG along with all the other LAG member ports.
- LACP parameters can be modified from the LACP tab.
- LAG member ports can be added from the LAG Members tab.
- A UNI policy can be applied to a LAG used as a SAP in a stacked VLAN from the Policies tab.
- An MVRP configuration and VLAN restriction can be applied to a LAG from the MVRP tab. If a port is a LAG member, you cannot modify parameters on the MVRP general tab on that physical port.
- Statistics, network interfaces, and fault information is available from the appropriate tabs.

26 Expand the LAG object in the navigation tree to view the created LAG groups and the unassigned dynamic LAG members group. Expand the LAG group object to view the subgroup member ports, the priority, and the LACP state. Expand the Unassigned Dynamic LAG Members group object to view dynamic LAG members that have not been assigned to a dynamic LAG group.

Procedure 14-13 To configure OmniSwitch dynamic LAG members

Perform the following procedure to add members to a dynamic LAG and modify existing dynamic LAG members.



Note 1 — LAG members are not added during the creation of the dynamic LAG, as they are with static LAGs. When a new dynamic LAG member is created it is placed into the Unassigned Dynamic LAG Members object. The new dynamic LAG members remain under the Unassigned Dynamic LAG Members object until the system identifies a LAG with matching properties. When an unassigned LAG member joins a LAG, the member is removed from the Unassigned Dynamic LAG Members object and added to the appropriate LAG object.

Note 2 — When a port is assigned to a LAG member, you cannot modify the port properties using the 5620 SAM.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure the LAG members and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Logical Groups icon.

4 Right-click on the Unassigned Dynamic LAG Members object and choose Create LAG Members from the contextual menu. The Create LAG Member - Only show compatible ports form appears.

5 Configure the Show Only Compatible Ports and Class parameters.

6 Click on the Next button. The Create LAG Member - Select Ports form opens.

7 Click on the Search button to display a list of compatible ports. Choose ports from the list to construct the LAG.

Add ports to the LAG as follows:

- Choose up to the maximum number of ports you require from the list of ports. You can select more than one port at a time from the list.
- Click on the Next button. The Specify the Member Properties form opens.



Note 1 — If there are no compatible ports to choose from and you want to edit some of the existing ports to be compatible, then disable the Show Only Compatible Ports parameter. Click on the Next button. Choose ports to edit from the list and click on the Properties button.

Note 2 — For all ports in an LAG, you must disable auto-negotiation, configure the same speed, and set the ports to full duplex. Mobile ports cannot be part of a LAG.

8 Configure the parameters:

- Priority
- System Id
- System Priority
- Admin Key
- Admin State

9 Click on the Finish button. The Create LAG - Wizard Completed form opens.

10 Enable the View the newly created interface check box if you need to view the LAG properties.

11 Click on the Close button to close the form.

12 If you need to modify a dynamic LAG member, go to step 13.

13 Right click on a LAG member and choose Properties from the contextual menu.

14 The LAG Member (edit) form opens on the General tab.

15 Configure the Priority parameter in the LAG Member panel, if required.

16 Configure parameters in the Actor panel, if required.

- System Id
- System Priority
- Admin Key
- Admin State

17 Configure parameters in the Partner panel, if required.

- Admin Key
- Admin System Id
- Admin Port
- Admin System Priority
- Admin Port Priority
- Admin State

18 Click on the OK button. A dialog box appears.

19 Click on the Yes button to save your changes and close the form.

20 Click on the Close button to close the form.

Procedure 14-14 To create a LAG link mapping profile

A LAG link mapping profile specifies the LAG egress port used by SAPs and interfaces associated with the profile, and what action the LAG should take if the assigned port fails.



Note — You can only use LAG link mapping profiles on an NE that is in chassis mode D or higher.

1 Create a LAG as described in Procedure 14-10, or configure a LAG as described in Procedure 14-11. Table 14-1 describes the required parameter values that must be set in order to use LAG link mapping profiles.

Table 14-1 LAG link mapping prerequisites

Tab	Parameter	Required values
General	Port Type	Access or Hybrid
Access	QoS Adaptation	Link
LAG Members	Sub-Group ID	All LAG members must be in the same sub-group.

2 Click on the Link Mapping Profiles tab in the LAG (edit) form.

3 Click on the Create button. The Link Mapping Profile (New Instance) form appears.

4 Configure the parameters on the General tab:

- ID
- Description
- Failure Mode

5 Click on the Mapping Profile Links tab.

6 Click on the Create button. The Link Mapping Profile Link (New Instance) form appears.

7 Click on the Select button. A list of LAG member ports appears.

8 Select a port from the list and click on the OK button. The selected port will be used for egress traffic for interfaces assigned to this LAG link mapping profile.

9 Configure the Type parameter.

10 Click on the OK button. The assigned port appears in the list.

11 Configure a secondary port by repeating steps 6 to 10, if required.

12 Assign the LAG link mapping profile to an interface or MSAP Policy by performing one of the following, if required:

a To assign the LAG link mapping profile to a network interface, access interface, or SAP, perform the following:

i Click on the Apply button.

ii Click on the Network Interface, L2 Access Interface, L3 Access Interface, or Service Access Points tab. A list of interfaces that terminate on the LAG appears.

iii Select an interface from the list, and click on the Properties button. The Interface (Edit) form appears.

iv Click on the Port tab.

v Click on the Select button beside the LAG Link Map Profile ID parameter. A list of LAG link mapping profiles appears.

vi Select a LAG link mapping profile and click on the OK button.

vii Click on the OK button. The Interface (edit) form closes.

b To assign the LAG link mapping profile to an MSAP policy, perform the following:

i Click on the Apply button.

ii From the 5620 SAM main menu, select Policies→Residential Subscriber. The Residential Subscriber Policies form appears.

iii Configure the filters and click on the Search button.

iv Select an MSAP policy from the list and click on the Properties button. The MSAP Policy (edit) form appears.

v Click on the Local Definitions tab.

vi Select the local definition for the site where the LAG link mapping profile is configured, and click on the Properties button. The MSAP Policy (Local Policy) form appears.

vii If the Distribution Mode parameter is set to Sync With Global, click on the Switch Mode button.

viii Set the LAG Link Map Profile parameter to the ID of the LAG link mapping profile you need to assign to the MSAP policy.

ix Click on the OK button.

x Close the MSAP Policy and Residential Subscriber Policies forms.

13 Click on the OK button. The new LAG link mapping profile appears in the list.

Procedure 14-15 To configure BFD on a LAG

1 Create a LAG as described in Procedure 14-10, or configure a LAG as described in Procedure 14-11.

2 Click on the BFD tab in the LAG (edit) form. A list of BFD entries appears.

3 Select the IPv4 or IPv6 entry and click on the Properties button. The BFD Configuration on LAG form appears.

4 Configure the parameters on the LAG tab:

- Family
- BFD State
- BFD on Distributing Links Only
- Multiplier
- Max Admin Down Time
- Max Setup Time
- Transmit Interval
- Receive Interval
- Local IP Address
- Remote IP Address

5 Click on the OK button. The BFD Configuration on LAG form closes.

Procedure 14-16 To view micro-BFD sessions on a LAG

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the LAG object that you want to configure. The path is Network→*NE*→Logical Groups→LAGs→LAG *n*.

3 Right-click on the LAG *n* icon and choose Properties. The LAG (Edit) form opens with the General tab displayed.

4 Click on the BFD tab in the LAG (edit) form. A list of BFD entries appears.

5 Select the IPv4 or IPv6 entry and click on the Properties button. The BFD Configuration on LAG form appears.

6 Click on the Micro BFD Session tab. A list of BFD sessions associated with the LAG appears.

7 Select a BFD session and click on the Properties button to view information about the selected session.

15 — Shelf object configuration

15.1 Shelf object configuration overview *15-2*

15.2 Working with shelf objects *15-2*

15.3 Working with card and card slot objects *15-6*

15.4 Working with daughter card objects *15-9*

15.5 Working with bundle objects *15-10*

15.6 Workflow to manage shelf objects *15-12*

15.7 Shelf object configuration procedures *15-14*

15.8 Card and card slot object configuration procedures *15-38*

15.9 Daughter card slot object configuration procedures *15-47*

15.10 Bundle configuration procedures *15-59*

15.1 Shelf object configuration overview

In the equipment navigation tree, shelf objects are children of device objects. They appear below logical group objects in the navigation tree. Card slot objects are children of shelf objects, and as such appear below the shelf object in the navigation tree. Daughter card slot objects are created in the navigation tree as children of the card slot object, after the card slot object is configured. APS bundle objects appear below the shelf object and Bundle objects appear below daughter card objects that are configured as channelized MDAs.

This chapter contains the procedures to configure shelf, card slot, daughter card slot, and bundle objects using the navigation tree. See chapter 5 for more information about using the navigation tree. See chapter 34 for more information about APS bundles.

15.2 Working with shelf objects

Shelf objects represent the hardware that is configured on a shelf. When you choose the shelf object in the navigation tree and click on Properties in the contextual menu, you can view the states and conditions of the shelf including:

- general information
- fan tray state and speed
- power supply tray statuses
- LED statuses
- card slots
- hardware environment information
- CCM properties
- PoE
- timing
- statistics
- dry contacts
- faults
- port segregation
- software control module
- software bank information
- cross connects

The Display tab displays a graphical representation of the device's shelf and its equipment components, such as the empty card slots and the cards that are installed on the device. You can double-click on an object under this tab to open its Properties configuration form. Right-click on the object and you have full access to the contextual menus for the object and any child objects, for example the ports of a card (dynamic graphical representation only).

Chassis modes

The chassis mode of a device indicates the minimum IOM or IMM card type that is initialized by the device and determines the scaling numbers and features that are available to the system. The chassis mode can be configured on the following device types:

- 7450 ESS-4, 7450 ESS-6, 7450 ESS-7, and 7450 ESS-12
- 7450 ESS-6v
- 7750 SR-7 and 7750 SR-12

See the appropriate device Release Notice for scaling information.



Note — Chassis modes are not supported on the 7950 XRS.

Tables 15-1 and 15-2 list the chassis modes that you can configure on each IOM and IMM card type for the supported devices.

Table 15-1 Chassis modes and 7750 SR IOM and IMM card compatibility

Card	Chassis mode	NE release
2 x 10-Gig MDA IOM	A	All supported releases
2 x 10-Gig MDA IOM Card, B	A and B	
2 x 10-Gig MDA IOM 2	A, B, and C	
2 x XP MDA IOM 3	A, B, C, and D	
2 x XP MDA IOM 3, B	A, B, C, and D	9.0 R6 or later
4-Port 10 GE XFP IMM	A, B, C, and D	All supported releases
8-Port 10 GE XFP IMM		
48-Port GIGE SFP IMM		
48-Port GIGE SFP IMM, B		9.0 R6 or later
48-Port GIGE TX IMM		All supported releases
48-Port GIGE TX IMM, B		9.0 R6 or later
12-Port 10GE SFP IMM		8.0 R5 or later
1-Port 100GE CFM IMM		
3-Port 40GE QSFP possibly oversubscribed IMM		9.0 R4 or later

Table 15-2 Chassis modes and 7450 ESS IOM card compatibility

Card	Chassis mode	7450 ESS-7, 7450 ESS-12, and 7450 ESS-4	7450 ESS-6	7450 ESS-6v
2 x 10-Gig MDA IOM	A	All supported releases	All supported releases	All supported releases
2 x 10-Gig MDA IOM Card, B	A and B			
2 x 10-Gig MDA Oversubscribed IOM	A and B	8.0 and 9.0	8.0 and 9.0	8.0 and 9.0
2 x XP MDA IOM 3	A, B, and B	All supported releases	All supported releases	All supported releases

(1 of 2)

Card	Chassis mode	7450 ESS-7, 7450 ESS-12, and 7450 ESS-4	7450 ESS-6	7450 ESS-6v
2 x XP MDA IOM 3, B	A, B, C, and D	9.0 R6 or later	9.0 R6 or later	9.0 R6 or later
48-Port GIGE SFP IMM		All supported releases	All supported releases	All supported releases
48-Port GIGE SFP IMM, B		9.0 R6 or later	9.0 R6 or later	9.0 R6 or later
48-Port GIGE TX IMM		All supported releases	All supported releases	All supported releases
48-Port GIGE TX IMM, B		9.0 R6 or later	9.0 R6 or later	9.0 R6 or later
3-Port 40GE QSFP possibly oversubscribed IMM		9.0 R4 or later	—	—

(2 of 2)

Timing synchronization

Timing synchronization parameters can be configured on 7210 SAS, 7450 ESS, 7705 SAR, 7705 SAR-H, 77710 SR, 7750 SR, 7750 SR-c4, 7750 SR-12E, 7750 SR-c12, and 7950 XRS shelves that contain the following daughter cards:

- 10 Gigabit Ethernet with 2- and 4-port configurations
- 10/100/1000 Ethernet SFP with 20 ports
- 10 Gigabit Ethernet XFP with 4-, 8-, and 48-port configurations
- 10-port Gigabit Ethernet SFP HA
- 16 x Channelized DS1/E1 ASAP
- 16 x Channelized DS1/E1 ASAP v2
- 8-port Ethernet
- 8-port Ethernet v2
- 4-port OC3/STM1 ASAP SFP
- 4 X MWA Gig Ethernet (2 TX, 2 SFP) + 4 X Gig Ethernet SFP
- 8-port GIGE SPF card V2 (-48/+24 VDC)
- 2-port 100 Gigabit Ethernet CFP C-XMA
- 20-port 10 Gigabit Ethernet SFP + C-XMA
- 40-port 10 GE SFP+ XMA
- 4-port 100 GE CXP XMA
- 2-port OC-192c/STM-64c XFP MDA

See Procedure 15-7 for more information about configuring timing synchronization.

IEEE 1588 PTP clock

The 5620 SAM supports IEEE 1588 PTP clocks for packet-based timing synchronization from a master clock to one or more slave clocks in a network. You can configure IEEE 1588 PTP clocks on the following NEs:

- 7210 SAS-D ETR
- 7210 SAS-M
- 7210 SAS-X
- 7450 ESS
- 7705 SAR
- 7705 SAR-A
- 7705 SAR-H
- 7705 SAR-W
- 7705 SAR-M/ME
- 7710 SR
- 7750 SR
- 7750 SR-c4
- 7750 SR-12E
- 7750 SR-c12

Depending on the device, NEs can be configured with an ordinary master, ordinary slave, or boundary clock. The 7705 SAR-A, 7705 SAR-M/ME and the 7705 SAR-W, can also be configured with a transparent clock.

Synchronization management

You can use the 5650 CPAM to manage synchronization domains and assign IP path monitors to PTP peers. See "Synchronization management" in the *5650 CPAM User Guide* for more information.

Time of Day management on the 7705 SAR-H

The 7705 SAR-H provides Time of Day information using unmodulated (B000) or modulated (B12X) formats using an RJ45 connector. Only output operations are supported on the 5620 SAM.

SNTP Time Synchronization

The 7705 SAR-H supports Simple Network Time Protocol (SNTPv4). It is a compact, client-only version of NTP. It can receive time from SNTP and NTP servers.

SNTP provides time accuracy within 100 ms of the time source. SNTP can only receive the time from NTP servers; it is not used to provide time services to other systems. SNTP does not authenticate traffic.

The 7705 SAR-H supports SNTP in both uni-cast client modes (point-to-point) and broadcast client modes (point-to-multipoint).

IEEE1588 Time Synchronization

The 7705 SAR-H supports Precision Timing Protocol as defined in IEEE1588v2. The slave capability allows for the transfer to the Time of Day for a 1588 grand master or master clock. The accuracy based on this method can achieve sub-microsecond stability, which is superior to NTP or SNTP. This accuracy is used for OAM 1-way latency measurements.

Power management on the 7950 XRS

The 5620 SAM supports configuring power management zones on 7950 XRS nodes, and power priority values on MDA cards installed on 7950 XRS nodes. Each MDA and APEQ provisioned on 7950 XRS nodes is associated with a power management zone, and during startup MDAs with higher power priority values are started first. You can view information and collect statistics about power availability and shedding using the 5620 SAM.

See Procedure 15-21 for information about configuring a power management zone. See Procedure 15-33 for information about configuring power priority values on an MDA. See the *5620 SAM Statistics Management Guide* for information about gathering power statistics using the 5620 SAM.

Detailed information about power usage is available on the power management zone, shelf, card slot, and daughter card slot configuration forms for 7950 XRS nodes. Use the Hardware Environment tab to view information about power usage.

15.3 Working with card and card slot objects

When you click on the plus sign beside a shelf object, the card slots in the shelf appear in the navigation tree. They can appear as empty card slots when a card is not provisioned for the slot.

Card slot objects for the OS 6250, OS 6400, OS 6450, OS 6850, OS 6850E, and OS 6855 appear automatically when a physical device exists because the entire device is represented by a card slot object and no daughter cards are associated with these devices.

Card slots can be configured with CMM or Ethernet card types for the OS 9600, OS 9700, OS 9800, OS 9700E, and OS 9800E devices, but there are no daughter cards associated with these devices.

When the 5620 SAM discovers a 7210 SAS or 7705 SAR-F, the integrated IOM and daughter card objects appear automatically in the navigation tree.

When the 5620 SAM discovers a supported PAC FP3 IMM in a card slot, the daughter cards and ports appear automatically in the navigation tree. Daughter cards and ports that are discovered in this way cannot be manually deleted.

Choose Configure Card from the contextual menu of the object and assign a supported card type for the slot. The Assigned Card Type parameter lists the card types can be assigned to the card slots.

Some card types can be pre-provisioned in a slot before the card is installed in the chassis. A card and daughter card must be provisioned before a port can be configured.

When a card is first configured, the administrative state can be down. The resource is not operationally up until the card is equipped and the administrative state is up. A card can only be provisioned in a slot that is vacant, and no other card can be provisioned (configured) for that specific slot.

To reconfigure a slot position, delete the card currently in the slot and configure the new card type added to the slot. A card can only be provisioned in a slot when the card type is allowed in the slot.



Note — You can also reconfigure a slot position by changing the chassis mode. The chassis mode determines the minimum card requirements. See section 15.2 for more information about chassis modes.

For example, if a 2 x 10-Gig MDA IOM 2 card is installed in the chassis that is running in chassis mode B, the card behaves as a 2 x 10-Gig MDA IOM Card, B. You can upgrade the chassis mode to C to make the IOM card behave as a 2 x 10-Gig MDA IOM 2 card.

You can configure forwarding plane properties on the properties forms for IOM 3, IMM, and XCM cards. IOM 3 and IMM cards support one forwarding plane, and XCM cards support two forwarding planes — one for each XMA card slot.



Note 1 — You cannot configure a forwarding plane on an XCM card until you have provisioned the corresponding XMA card.

Note 2 — You cannot remove a provisioned XMA card when any of the following is true on the corresponding XCM forwarding plane:

- Egress WRED queue control is administratively enabled
- Access ingress queue groups are configured
- Network ingress queue groups are configured
- The Dynamic Enforcement Policer Pool Size parameter is configured with a nonzero value

Card provisioning and chassis modes

The behavior of the installed card depends on the chassis mode that has been configured on the device. Table 15-3 describes the behavior of the provisioned (configured) card types and installed cards in each chassis mode.

Table 15-3 Behavior of installed IOM cards

Provisioned card type	Installed card type	Behavior
2 x 10-Gig MDA IOM	2 x 10-Gig MDA IOM	The IOM card appears and behaves at the scaling limits of the 2 x 10-Gig MDA IOM.
	2 x 10-Gig MDA IOM Card, B	The IOM card appears and behaves as a 2 x 10-Gig MDA IOM. The 2 x 10-Gig MDA IOM Card, B is fully backward-compatible with the 10-Gig MDA IOM.
	2 x 10-Gig MDA IOM 2	The IOM card appears and behaves as a 2 x 10-Gig MDA IOM. The 2 x 10-Gig MDA IOM 2 is fully backward-compatible with the 10-Gig MDA IOM.
	2 × XP MDA IOM 3 (1)	The IOM card appears and behaves as a 2 x 10-Gig MDA IOM. The 2 x XP MDA IOM is fully backward-compatible with the 10-Gig MDA IOM.

(1 of 3)

Provisioned card type	Installed card type	Behavior
2 x 10-Gig MDA IOM Card, B	2 x 10-Gig MDA IOM	The IOM card fails because the minimum card requirements are not met.
	2 x 10-Gig MDA IOM Card, B	The IOM card appears and behaves at the scaling limits of the 2 x 10-Gig MDA IOM Card, B.
	2 x 10-Gig MDA IOM 2	The IOM card appears and behaves as a 2 x 10-Gig MDA IOM Card, B. The 2 x 10-Gig MDA IOM 2 is fully backward-compatible with the 10-Gig MDA IOM Card, B.
	2 × XP MDA IOM 3 (1)	The IOM card appears and behaves as a 2 x 10-Gig MDA IOM Card, B. The 2 x XP MDA IOM 3 is fully backward-compatible with the 10-Gig MDA IOM Card, B.
2 x 10-Gig MDA IOM 2	2 x 10-Gig MDA IOM	The IOM card fails because the minimum card requirements are not met.
	2 x 10-Gig MDA IOM Card, B	The IOM card fails because the minimum card requirements are not met.
	2 x 10-Gig MDA IOM 2	The behavior of the card depends on the operational chassis mode: • 2 x 10-Gig MDA IOM in chassis mode A • 2 x 10-Gig MDA IOM Card, B in chassis mode B • 2 x 10-Gig MDA IOM 2 in chassis mode C and D
	2 × XP MDA IOM 3 (1)	The behavior of the card depends on the operational chassis mode: • 2 x 10-Gig MDA IOM in chassis mode A • 2 x 10-Gig MDA IOM Card, B in chassis mode B • 2 x 10-Gig MDA IOM 2 in chassis mode C and D
2 × XP MDA IOM 3 card (1)	2 x 10-Gig MDA IOM	The IOM card fails because the minimum card requirements are not met.
	2 x 10-Gig MDA IOM Card, B	The IOM card fails because the minimum card requirements are not met.
	2 x 10-Gig MDA IOM 2	The IOM card fails because the minimum card requirements are not met.
	2 × XP MDA IOM 3 (1)	The behavior of the card depends on the operational chassis mode: • 2 x 10-Gig MDA IOM in chassis mode A • 2 x 10-Gig MDA IOM Card, B in chassis mode B • 2 x 10-Gig MDA IOM 2 in chassis mode C • 2 x XP MDA IOM 3 in chassis mode D. With mixed mode enabled for 7750 SR, only the IPv6 features of the IOM3 card are enabled, but no other IOM3 features are available.

(2 of 3)

Provisioned card type	Installed card type	Behavior
2 × XP MDA IOM 3, B card [(1)]	2 x 10-Gig MDA IOM	The IOM card fails because the minimum card requirements are not met.
	2 x 10-Gig MDA IOM Card, B	The IOM card fails because the minimum card requirements are not met.
	2 x 10-Gig MDA IOM 2	The IOM card fails because the minimum card requirements are not met.
	2 × XP MDA IOM 3 [(1)]	The behavior of the card depends on the operational chassis mode: • 2 x 10-Gig MDA IOM in chassis mode A • 2 x 10-Gig MDA IOM Card, B in chassis mode B • 2 x 10-Gig MDA IOM 2 in chassis mode C • 2 x XP MDA IOM 3 in chassis mode D. With mixed mode enabled for 7750 SR, only the IPv6 features of the IOM3 card are enabled, but no other IOM3 features are available.

(3 of 3)

Note
(1) Also applies to any IMM

15.4 Working with daughter card objects

After the card is created in the card slot you can create and configure MDAs, also known as daughter card objects, in the daughter card slot that appears when you click on the plus sign beside the card object. The daughter card slots in the card appear in the navigation tree. They appear as empty daughter card slots when a daughter card is not provisioned for the slot. When a daughter card is provisioned for the slot, it is identified.

See the appropriate device section in chapter 8 for device-specific daughter card information.

A 5620 SAM license allows the management of a specific number of MDAs for each device type. You can purchase additional MDA capacity as required. MDAs fall into two licensing categories: premium and standard. Generally, non-high-performance MDA cards are considered standard. All IMM, HSMDA, XMDA, and XP MDA cards are premium.

Each IMM card is associated with a platform, and counts towards the licensed IMMs for that platform regardless of where it is installed. For example, a 7750 SR IMM installed on a 7450 ESS is counted as a premium 7750 SR MDA for the purposes of licensing. Enabling or disabling mixed mode does not change the associated platform type of a card.

Note — After the 5620 SAM discovers the number of premium MDAs allowed by the license, the 5620 SAM can no longer discover 7705 SAR-8, 7705 SAR-18, 7710 SR, and 7450 ESS devices.

IMM daughter cards

The IMM card integrates IOM 3 and high bandwidth MDA functionality on a single card that fits into existing IOM slots. When you configure the IMM the integrated MDAs are automatically configured. The 5620 SAM equipment tree displays the IMM with two daughter cards, each having half of the total number of ports supported by the IMM.

Each daughter card object contains a number of ports that are specific to the type of service required. The port objects are created automatically under the daughter card but they must be configured based on the function served by the port; for example, as an access interface for a VPRN service.

You can associate policies to daughter cards. Network buffer policies are used to create and edit QoS buffer pool resources on egress network ports, channels, and ingress ports. Ingress and egress network ports and channels have a dedicated buffer pool for egress queuing. The ingress and egress network traffic is handled by a buffer pool at the ingress and a buffer pool at the egress.

You can also configure multicast path management on an IMM daughter card. See chapter 45 for more information.

MDA modes for the 7705 SAR

The 5620 SAM allows you to configure the MDA mode of some MDA types on the 7705 SAR. The MDA mode on a channelized ASAP determines the capabilities that are available to the MDA. The MDA mode on an XMDA determines the number of ports that are available to the MDA. See the MDA Mode parameter description for more information.

15.5 Working with bundle objects

Bundle objects can be configured as multilink PPP, IMA group, or FR group bundles. Multilink PPP, IMA group, and FR group bundles appear as Bundle objects under the daughter card object if the daughter card has been configured as a channelized MDA.

APS Bundle objects appear in the navigation tree as children of the shelf object. APS Bundle objects are configured to protect multilink PPP and IMA bundles on channelized ASAP MDAs. See chapter 34 for more information on APS and APS bundles.

Multilink PPP bundles

You can create multilink PPP bundles to:

- bundle DS0 channels together to be used as a SAP
- provide a mechanism to distribute data across multiple links to achieve higher bandwidth

The following general rules apply to multilink bundles.

- Table 15-4 lists the maximum number of multilink bundles that can be created on each MDA.
- DS0 channels can be aggregated on a single MDA only.
- Up to 8 members can be added to a bundle.
- The Encap Type parameter of a member cannot be set to FR.
- A DS0 channel can host only one SAP.
- If a channel is being used as a SAP, it cannot be added to a bundle.

Table 15-4 Multilink bundle configuration maximum

MDA	Bundle maximum
All MDAs other than channelized ASAP MDAs	56
• 1 x OC12 Deep Channel • 4 x OC3 Deep Channel • 12 x DS3/E3 Deep Channel • 4 x DS3/E3 Deep Channel • 8 x DS1/E1 Channel CMA (7710 SR)	56
4 x Channelized DS3/E3 ASAP MDA	112
• 4 x Channelized OC3 ASAP • 1 x Channelized OC12 ASAP • 12 x Channelized DS3/E3 ASAP	256

See Procedure 15-41 to create a multilink PPP bundle.

IMA group bundles

IMA group bundles combine ATM-encapsulated DS0 channel groups into a single ATM interface. The following general rules apply to IMA group bundles.

- IMA group bundles can only be created on:
  - channelized ASAP MDAs with SDH or SONET framing the 7750 SR or 7710 SR
  - ATM DS1/E1 CMA on the 7710 SR
  - channelized DS1/E1 ASAP daughter cards on the 7705 SAR
- The encapsulation type of the DS0 group channel must be ATM.
- The Clock Source parameter of the DS1 channel must be set to Node-Timed.
- Table 15-5 lists the maximum number of IMA group bundles that can be created on each MDA.
- IMA group members must be on the same MDA.

Table 15-5 IMA group bundle configuration maximums

Device	MDA	Bundle maximum
7750 SR	All MDAs other than channelized ASAP MDAs	56

(1 of 2)

Device	MDA	Bundle maximum
7750 SR 7710 SR	4 x Channelized DS3/E3 ASAP MDA	112
7750 SR 7710 SR	• 4 x Channelized OC3 ASAP • 1 x Channelized OC12 ASAP • 12 x Channelized DS3/E3 ASAP	256
7710 SR	8 x ATM DS1/E1 CMA	8
7705 SAR	16 x Channelized DS1/E1 ASAP	8
7705 SAR	2 x Channelized OC3/STM1 ASAP	16

(2 of 2)

See Procedure 15-39 to create a multilink PPP bundle.

FR group bundles

FR group bundles are used to fragment lower priority DLCI frames to minimize jitter and delay on higher priority DLCI frames. The following general rules apply to FR group bundles.

- FR group bundles can only be created on channelized ASAP MDAs.
- FRF12 cannot be enabled on a SAP that is using an FR group bundle.
- DS0 channel groups must have all their timeslots selected and have their encapsulation type set to FR to be configured as bundle members.



Note — You can configure a maximum of 128 FR group bundles on an MDA.

See Procedure 15-37 to create a multilink PPP bundle.

15.6 Workflow to manage shelf objects

The following workflow describes the sequence of high-level tasks required to manage and configure shelf objects and shelf object children. This workflow assumes that the physical devices have been installed, commissioned, and discovered. See chapter 9 for more information about device commissioning. See chapter 10 for more information about device discovery.



Note — Shelf objects and shelf object children can be accessed using the equipment navigation tree. See chapter 5 for more information about using the equipment navigation tree.

1 As required, perform the following procedures to configure shelf objects.

   a Configure the chassis mode of a device. See Procedure 15-1.

   b Configure dry-contact sensor monitoring. See Procedure 15-3.

c Configure switch fabric multicast ingress replication rates. See Procedure 15-4.

d Configure IMPM overrides. See Procedure 15-5.

e Enable mixed mode on a 7450 ESS or 7750 SR device. See Procedure 15-6.

f Configure timing synchronization. See Procedure 15-7.

g Configure the IEEE 1588 clock on a 7705 SAR. See Procedure 15-8.

h Configure the IEEE 1588 PTP port on a 7705 SAR. See Procedure 15-9.

i Configure NTP on supported device types. See Procedure 15-10.

j Configure a 7705 SAR microwave link. See Procedure 15-11.

k Configure a 7705 SAR MW link member. See Procedure 15-12.

l Configure auxiliary alarm definitions on a 7705 SAR. See Procedure 15-13.

m Configure the IEEE 1588 PTP clock on supported devices. See Procedure 15-14.

n Configure the IEEE 1588 PTP peer on supported devices. See Procedure 15-15.

o Manage OmniSwitch running configuration. See Procedure 15-16.

p Configure OmniSwitch health monitoring. See Procedure 15-17.

q Configure a CCM on a 7950 XRS-20. See Procedure 15-18.

r Configure power supply trays. See Procedure 15-20.

s Configure power management zones on a 7950 XRS. See Procedure 15-21.

2 Assign a card type to a chassis slot. See Procedure 15-23.

3 As required, configure the card and card slot objects as follows:

a Configure an egress WRED queue control on an IOM 3 or IMM forwarding plane. See Procedure 15-24.

b Configure IMPM on a 2 × XP MDA IOM 3 or IMM forwarding plane. See Procedure 15-25.

c Enable named pool mode. See Procedure 15-28.

d Configure OmniSwitch stacks. See Procedure 15-30.

e Configure an OmniSwitch CPU temperature threshold. See Procedure 15-31.

f Configure a CPM on a 7950 XRS. See Procedure 15-32.

4 As required, configure daughter card objects as follows:

a Configure an MDA. See Procedure 15-33.

b Configure IMPM on an MDA. See Procedure 15-34.

c View operational multicast channel properties on an MDA. See Procedure 15-35.

d Configure a module card on the 7705 SAR-M/ME. See Procedure 15-36.

5 As required, create or modify bundle objects as follows:

a Multilink PPP bundle. See Procedures 15-41 and 15-42.

b IMA group bundle. See Procedures 15-39 and 15-40.

c FR group bundle. See Procedures 15-37 and 15-38.

d MLPPP bundle as a network interface on a channelized ASAP MDA. See Procedure 15-44.

15.7 Shelf object configuration procedures

Use the following procedures to configure shelf objects using the navigation tree.

Procedure 15-1 To configure the device chassis mode

Perform this procedure to configure the chassis mode for the device. See chapter 12 for more information about chassis modes.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the shelf object on which you want to configure the chassis mode. The path is Network→*NE*→Shelf.

3 Right-click on the Shelf object and choose Properties. The Shelf (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- Administrative Mode
  If you downgrade the administrative chassis mode, the device must be rebooted to change the operational chassis mode.
- Force Mode
  Forcing a chassis mode change does not change the operational chassis mode unless there is a compatible card type equipped on the device. See chapter 12 for more information about the minimum card type that must be installed for each chassis mode.

5 Click on the OK button. The Shelf (Edit) form closes.

Procedure 15-2 To configure a VWM shelf for a 7210 SAS

The 1830 VWM is an add-on optical module that attaches to the USB port of a 7210 SAS-E, 7210 SAS-M, or 7210 SAS-X, Release 5.0 R4 or later. Perform this procedure to create an equipment shelf that identifies the 1830 VWM module. You can create one VWM shelf per NE. See the 7210 SAS documentation.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the VWM Shelves object. The path is Network→NE→VWM Shelves.

3 Right-click on VWM Shelves and choose Configure VWM Shelf from the contextual menu. The VWM Shelf (Create) form opens.

4 Configure the parameters:

- Administrative State
- Shelf ID

You must configure the Shelf ID parameter with the hardware shelf ID value that is pre-set on the rotary dial of the 1830 VWM module. The Shelf ID parameter value must be an integer from 1 to 7.



Note — If the Shelf ID parameter does not match the hardware shelf ID, the correct manufacturer details do not appear on the VWM Shelf form.

5 Click on the OK button. The VWM Shelf (Create) form closes.

Procedure 15-3 To configure 7210 SAS dry contact sensors

Perform this procedure to configure dry contact sensors on a 7210 SAS-E, 7210 SAS-M, 7210 SAS-T, or 7210 SAS-X.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the shelf object on which you want to configure dry contact sensors. The path is Network→*NE*→Shelf.

3 Right-click on the Shelf object and choose Properties. The Shelf (Edit) form opens with the General tab displayed.

4 Click on the External Alarms tab. The Shelf Dry Contacts tab is displayed.

5 Choose one of the dry contacts and click on the Properties button. The DryContact (Edit) form opens.

6 Configure the parameters:

- Name
- Description
- Monitored Status
- Polarity
- Alarm Severity
- Alarm Trigger Message
- Alarm Clear Message
- Control Status
- Control Type
- Connected To

7 Click on the OK button to close the DryContact (Edit) form.

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button. The Shelf (Edit) form closes.

Procedure 15-4 To configure switch fabric multicast ingress replication rates

Perform this procedure to configure the total multicast replication rates for primary and secondary ingress paths for each switch fabric multicast plane.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the shelf object on which you want to configure switch fabric multicast ingress replication rate. The path is Network→*NE*→Shelf.

3 Right-click on the Shelf object and choose Properties. The Shelf (Edit) form opens with the General tab displayed.

4 Click on the Multicast tab.

5 Configure the parameters:

- Primary Multicast Bandwidth (mbps)
- Secondary Multicast Bandwidth (mbps)
- Primary Multicast Bandwidth for Dual-SFM Mode (mbps)
- Secondary Multicast Bandwidth for Dual-SFM Mode (mbps)

6 Click on the OK button. The Shelf (Edit) form closes.

Procedure 15-5 To configure IMPM overrides

Perform this procedure to configure IMPM overrides. See Procedure 15-25 to configure IMPM on an IOM or XCM. See chapter 45 for more information on multicast path management.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the shelf object on which you want to configure MMRP IMPM overrides. The path is Network→*NE*→Shelf.

3 Right-click on the Shelf object and choose Properties. The Shelf (Edit) form opens with the General tab displayed.

4 Click on the Multicast tab.

5 Configure the parameters:

- Administrative Mode
- Round-Robin Inactive Records



Note — The Operational Mode parameter is not configurable. If the Administrative Mode parameter is changed, the value of the Operational Mode parameter changes to indicate the same mode as the Administrative Mode parameter after the system is rebooted.

6 Click on the OK button. The Shelf (Edit) form closes.

Procedure 15-6 To enable mixed mode

Perform this procedure to enable mixed mode on a 7450 ESS or 7750 SR. Enabling mixed mode on a 7450 ESS-6, 7450 ESS-6v, 7450 ESS-7, or 7450 ESS-12, enables the support of features on the IOM3-XP and associated MDA-XPs or IMMs.

Release 9.0 and later 7750 SR-7 and 7750 SR-12 devices support mixed mode, which allows you to enable IPv6 on a 7750 SR in chassis mode A or B without having to upgrade the entire chassis. Slots with network ports, and ports that require IPv6 support, can then be selectively upgraded for IOM3-XPs or IMMs.



Note — On Release 9.0 R5 and later 7750 SR-7 and 7750 SR-12 devices, mixed mode cannot be enabled when an ISA TMS MDA is provisioned.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the shelf object on which you want to enable mixed mode. The path is Network→*NE*→Shelf.

3 Right-click on the Shelf object and choose Properties. The Shelf (Edit) form opens with the General tab displayed.

4 Enable the Mixed Mode State on Chassis Enabled parameter.

5 Click on the OK button. The Shelf (Edit) form closes.

Procedure 15-7 To configure timing synchronization

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the shelf object on which you want to configure timing synchronization. The path is Network→*NE*→Shelf.

3 Right-click on the Shelf object and choose Properties. The Shelf (Edit) form opens with the General tab displayed.

4 Click on the Timing tab.

5 Configure the parameters, as required:



Note — The displayed parameters vary depending on the NE type, release, and the settings of other parameters.

- Reference Input Mode
- Reference Input Mode (revertive)
- Quality Level Reference
- First Timing Reference Input
- Second Timing Reference Input
- Third Timing Reference Input
- Fourth Timing Reference Input
- Type
- Interface Name
- Port or Channel Name
- Administrative State
- Quality Level Override
- First Timing Reference PTP Clock
- Second Timing Reference PTP Clock
- Role
- Wait to Restore Time (Min):
- Wait to Restore Time (Secs):
- Interface Type
- Input Administrative State
- Output Administrative State
- Output Line Length
- SSM
- Input Type
- Impedance Type
- Output Type
- Status
- Primary Reference Type
- Secondary Reference Type
- Sync In Port
- Sync Out Port

You must enable the Synchronous Ethernet parameter on the daughter card in order to configure the Timing Reference One and Timing Reference Two panels for SyncE. See Procedure 15-33.

When you select a port as a timing reference for SyncE, the Port Clock Mode parameter for the port must be set to Manual Slave. See Procedure 16-1. Other restrictions may also apply for SyncE port selection, depending on the device. See the NE documentation for more information.

For the 7210 SAS-D ETR, 7210 SAS-M, and 7210 SAS-X, PTP and SyncE are mutually exclusive. Consider the following when configuring timing synchronization on these 7210 SAS NEs:

- You can only choose PTP as an option for First Timing Reference Input when the Administrative State parameter in the PTP panel is set to Up.
- You cannot configure the Second Timing Reference Input parameter when the First Timing Reference Input parameter is set to PTP.
- You can only set the Administrative State parameter in the PTP panel to Up when the Administrative State parameter in both the Timing Reference One and Timing Reference Two panels is set to Down.
- You can only set the Administrative State parameter in the Timing Reference One and Timing Reference Two panels to Up when the Administrative State parameter in the PTP panel is set to Down.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The Shelf (Edit) form closes.

Procedure 15-8 To configure a 7705 SAR IEEE 1588 PTP clock

Perform this procedure to configure the IEEE 1588 PTP clock on a 7705 SAR that is configured as an IEEE 1588 PTP client: See Procedure 15-7 for information about how to configure a 7705 SAR as a PTP client.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the NE object on which you want to configure the IEEE 1588 PTP clock. The path is Network→*NE*.

3 Right-click on the NE and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 Click on the IEEE PTP Clock tab.

5 Click on the Create button. The IEEE 1588 PTP Clock (Create) form opens.

6 Configure the parameters:

- Clock Index
- Clock Type
- Clock Slave Only
- Admin State
- PTP Profile
- Dynamic Peers
- Clock Priority 1
- Clock Priority 2
- Domain
- Frequency Source
- Clock Time Reference Priority

7 Click on the Select button beside the Clock MDA parameter and choose a source MDA for the PTP clock.

8 Click on the Select button beside the Interface Name parameter and choose a source interface for the PTP clock.

9 Click on the Apply button. A dialog box opens.

10 Click on the OK button.

11 As required, turn up PTP ports on the IEEE 1588 PTP clock.

i Choose a PTP port from the PTP Port panel and click on the Properties button. The IEEE 1588 PTP Port (Edit) form opens with the General tab displayed.

ii Configure the Admin State parameter.

iii Click on the OK button. The IEEE 1588 PTP Port (Edit) form closes.

12 Click on the OK button. A dialog box appears.

13 Click on the OK button. The IEEE 1588 PTP Clock (Create) form closes.

14 Click on the OK button. The Network Element (Edit) form closes.

Procedure 15-9 To configure a 7705 SAR IEEE 1588 PTP port

Perform this procedure to configure the IEEE 1588 PTP port on a 7705 SAR that is configured as an IEEE 1588 PTP client. See Procedure 15-7 for information about how to configure a 7705 SAR as a PTP client.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the shelf object on which you want to modify the IEEE 1588 PTP port. The path is Network→*NE*→Shelf.

3 Right-click on the Shelf object and choose Properties. The Shelf (Edit) form opens with the General tab displayed.

4 Click on the Timing tab.

5 Click on the PTP Port Properties button. The PTP Port (Edit) form opens with the General tab displayed.

6 Configure the parameters:

- Master 1 Address
- Master 2 Address
- Announce Receive Timeout
- Announce Interval
- Sync Interval

7 Click on the Recovered Clock History Master One tab to view master 1 clock recovery statistics.

8 Click on the Recovered Clock History Master Two tab to view master 2 clock recovery statistics.

9 Click on the OK button. The PTP Port (Edit) form closes.

10 Click on the OK button to save the configuration and close the Shelf (Edit) form.

Procedure 15-10 To configure NTP on supported devices

Perform this procedure to configure NTP on an NE. NEs can act as NTP servers, clients, or peers.

NTP configuration is supported on the following device types:

- 7705 SAR, Release 5.0 R5 or later
- 7705 SAR-H, Release 5.0 R3 or later
- 7750 MG, Release 3.1 or later
- 7750 SR, Release 8.0 or later
- 7950 XRS, Release 10.0 or later
- 9500 MPR

The 7705 SAR acts only as an NTP client and not as an NTP server. The 7705 SAR does not support NTP on a VPRN service.



Note 1 — For the 9500 MPR, if the main and spare NTP servers are defined with the same IP address in NEtO, only the IP address for the main server will be displayed in the 5620 SAM. Main and primary NTP servers with the same IP address should be avoided.

Note 2 — For any failed operation related to NTP server addition or modification, you must close the current GUI session on the NTP tab and reopen it before proceeding. This action removes the failed entry from the GUI cache so that it is not applied again.

Note 3 — The tabs and parameters that are configurable vary depending on the NE.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Choose Network→*NE* where *NE* is the object on which you need to configure NTP.

3 Right-click on the NE and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 If you are configuring a 7705 SAR or 9500 MPR, click on the NTP tab and configure the NTP State parameter, then go to step 7.

You must set the NTP State parameter to Enabled in order to configure the remaining NTP parameters.

5 Configure the NTP parameters on the General tab:

- NTP State

You must set the NTP State parameter to Enabled in order to configure the remaining NTP parameters.

When you change the NTP State parameter from Disabled to Enabled, you must click on the Apply button and confirm the action in order to activate the NTP tab.

6 Click on the NTP tab. The General tab is displayed.

7 Configure the parameters:

- Authentication Check
- Admin State
- NTP Server
- Server Authenticate
- MDA Time Stamp

8 Click on the Authentication tab and perform the following:

i Click on the Create button. The Network Time Protocol Authentication (Create) form opens.

ii Configure the parameters:

- Authentication Key Id
- Authentication Key
- Authentication Key Type

The values of the Authentication Key Id and Authentication Key parameters must be the same on the reference clock server and the NE.

iii Click on the OK button. The Network Time Protocol Authentication (Create) form closes and a dialog box appears.

iv Click on the OK button. The authentication key appears on the Authentication form.

9 Click on the Server tab and perform the following:

i Click on the Create button. The Network Time Protocol Server (Create) form opens.

ii Configure the parameters, as required:

- PTP Server
- IP Address
- Authentication Key Id
- NTP Version
- Preferred Server



Note — When the PTP Server parameter is enabled, the IP Address parameter becomes non-configurable. The address that is displayed in that field is not the PTP server address, it is an internal reference.

The Authentication Key Id and NTP Version parameters are only displayed when the PTP Server parameter is not enabled.

iii Click on the OK button. The Network Time Protocol Server (Create) form closes and a dialog box appears.

iv Click on the OK button.

If you are configuring a 9500 MPR, go to step 15.

10 Click on the Peer tab and perform the following:

i Click on the Create button. The Network Time Protocol Peer (Create) form appears.

ii Configure the parameters:

- Peer Address
- Authentication Key Id
- NTP Version
- Preferred Peer

iii Click on the OK button. The Network Time Protocol Peer (Create) form closes and a dialog box appears.

iv Click on the OK button. The NTP peer server appears on the Peer form.

11 Click on the Broadcast tab and perform the following:

i Click on the Create button. The NTP Broadcast (Create) form opens.

ii Click on the Select button beside the Interface Name parameter and select a source interface.

iii Click on the OK button.

iv The Select Source Interface - NTP Broadcast form closes and the NTP Broadcast (Create) form reappears.

v Configure the parameters:

- Direction
- Authentication Key Id
- NTP Version
- Authenticate
- Time to Live

You can only set the Direction parameter to transmit if the NTP Server parameter is enabled in step 7.

When the value of the Direction parameter is set to transmit, the Authentication Key Id, NTP Version, and Time to Live parameters are displayed.

vi Click on the OK button. The NTP Broadcast (Create) form closes and a dialog box appears.

vii Click on the OK button. The broadcast source interface appears on the Broadcast form.

12 Click on the Multicast tab and perform the following:

i Click on the Create button. The NTP Multicast (Create) form opens.

ii Configure the parameters:

- Direction
- Authentication Key Id
- NTP Version
- Authenticate

When the value of the Direction parameter is set to transmit, the Authentication Key Id and NTP Version parameters are displayed.

iii Click on the OK button. The NTP Multicast (Create) form closes and a dialog box appears.

iv Click on the OK button.

13 Click on the Associations tab and perform the following to view the properties of the NTP associations, if required:

i Configure the filters and click on the Search button. A list of NTP-associated NEs appears.

ii Choose an NE and click on the Properties button. The Network Time Protocol Associations (View) form opens. You can view information about the status and mode of the NTP server.

iii Close the Network Time Protocol Associations (View) form.

14 Click on the Clients tab and perform the following to view the properties of the NTP clients, if required:

i Configure the filters and click on the Search button. A list of NTP clients appears.

ii Choose an NTP client and click on the Properties button. The Network Time Protocol Clients (View) form opens. You can view information about the status and mode of the NTP client.

iii Close the Network Time Protocol Clients (View) form.

15 Click on the OK button. A dialog box appears.

16 Click on the Yes button. The Network Element (Edit) form closes.

Procedure 15-11 To configure a 7705 SAR MW link

Perform this procedure to configure a microwave link on the 7705 SAR-8 or 7705 SAR-18. To support an MW link, the NE must be configured with 4 × MWA Gig Ethernet (2 TX, 2 SFP) + 4 × Gig Ethernet SFP daughter cards. See Procedure 15-33 for information about how to configure daughter cards.



Note — The 5620 SAM supports the creation of an MW link in 1+0 protection mode and 1+1 protection mode. You can only configure 1+1 protection if the NE is in network mode.

For information about the 7705 SAR and 9500 MPRe, see the 9500 MPRe 4.1.0 user documentation and the appropriate 7705 SAR 6.0 R1 hardware guides.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Choose Network→NE→*Shelf* where Shelf is the 7705 SAR shelf object on which you need to create an MW link.

3 Click on the shelf object to expand the tree view.

4 Right-click on the MW Links item and choose Create MW Link from the contextual menu. The Create MW Link (Create) form opens, with the General tab displayed.



Note — Up to 12 MW links are supported on the 7705 SAR, Release 5.0 R5, and up to 24 MW links are supported on the 7705 SAR, Release 6.0 R1 or later.

5 Configure the Description parameter, if required.

6 Click on the MW Link tab.

7 Configure the parameters in the Hold Time panel:

- Auto-Assign ID
- Hold Time Up (seconds)
- Hold Time Down (seconds)

8 Click on the States tab and configure the Administrative State parameter.

9 Click on the Protection tab and configure the Protection Scheme parameter.

If you choose the value One Plus One Hsb, the Protection form displays additional panels.

10 To configure 1+1 radio protection, configure the following:

i In the Equipment Protection Scheme panel, configure the parameters, if required:

- Revertiveness
- Main Operation
- Spare Operation

ii In the Radio Protection Scheme panel, configure the parameters, if required:

- Revertiveness
- Main Operation
- Spare Operation

iii In the Transmission Protection Scheme panel, configure the parameters, if required:

- Main Operation
- Spare Operation

11 Click on the OK button. The MW Link (Create) form closes and the new MW link appears under the MW Links item in the navigation tree.

12 To modify the MW Link properties, right-click on the MW link and choose Properties. The MW Link (Edit) form appears with the General tab displayed.

13 Click on the MW Link tab and configure the parameters in the Hold Time panel, if required.

- Hold Time Up (seconds)
- Hold Time Down (seconds)



Note — The Peer IP Address parameter in the Peer Info panel is read-only and is displayed as follows:

- When the 9500 MPRe is in standalone mode, the Peer IP Address displays 0.0.0.0.
- When the 9500 MPRe is in single NE mode, the Peer IP Address displays the IP address of the other end 9500 MPRe if the other end of the radio link terminates on a 9500 MPRe in standalone mode.
- When the 9500 MPRe is in single NE mode, the Peer IP Address displays the IP address of the other end 7705 SAR if the other end of the radio link terminates on a 9500 MPRe in single NE mode.
- The Peer IP Address changes only when the 7705 SAR discovers a new peer after the radio link is operationally up between both 9500 MPRes or when the 7705 SAR reboots.

14 Configure the Peer Discovery parameter in the Peer Discovery panel.

15 Click on the Statistics tab to view statistical information, if required.

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The MW Link (Edit) form closes.

Procedure 15-12 To configure a 7705 SAR MW link member

Perform this procedure to configure a 7705 SAR MW link member on the 7705 SAR-8 or 7705 SAR-18. To support an MW link and an MW link member, the NE must be configured with 4 × MWA Gig Ethernet (2 TX, 2 SFP) + 4 × Gig Ethernet SFP daughter cards. See Procedure 15-33 for information about how to configure daughter cards.

If you configured 1+1 HSB protection in Procedure 15-11, you can configure a main radio and a spare radio for each MW link. By default, the main radio assumes the active status and the spare radio assumes the standby status.

If you configured 1+1 HSB protection and you want to revert back to 1+0 protection, you must delete the spare radio. You cannot delete the main radio.

1+1 HSB protection is displayed on the 5620 SAM physical topology map. The protection state is shown on the links, and 1+1 links are grouped in a common link group. The expansion of links on the physical map displays eight links. See section 6.2 for more information about the 5620 SAM physical topology maps.

For information about the 7705 SAR and 9500 MPRe, see the 9500 MPRe 4.1.0 user documentation and the appropriate 7705 SAR 6.0 R1 hardware guides.

1 Choose Network→NE→Shelf→Card Slot n→Daughter Card Slot n→Port n/n/n where the port object is the port that you need to use for the MW link.



Note 1 — Only the first four ports on the MDA are microwave-aware.

Note 2 — If a port is associated with an MW link, the port cannot be used as a timing reference. Also, if a port is already being used as a timing reference, the port cannot be associated with an MW link member.

2 Right-click on a port and choose Properties. The Physical Port (Edit) form opens with the General tab displayed.

3 Configure the Encapsulation Type parameter to be Dot1 Q.

4 Configure the Mode parameter.



Note 1 — Setting the Mode parameter to Access allows you to later associate the MW link with an L2 or L3 access interface for services. Setting the Mode parameter to Access is the typical setting. Setting the parameter to Network allows you to associate the MW link with a network interface.

Note 2 — 1+1 HSB radio protection can only be configured on a port in Network mode.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Physical Port (Edit) form closes.

7 Create an MW link member:

a If you configured 1+0 radio protection in Procedure 15-11, right-click on the MW link you created and choose Create MW Link Member. The Create MW Link Member step form opens.

b If you configured 1+1 HSB radio protection in Procedure 15-11, right-click on the MW link you created and choose Create MW Link Main Radio. The Create MW Link Member step form opens.

8 Configure the parameters on the Specify the Member Properties form, as required:

- Radio Name
- StandAlone
- Database Filename

The Database Filename must be the same name as the database file in the config file of the cflash directory and must be in a *.tar format.

9 Click on the Next button. The Select Ports form opens.

10 Choose the port from the list and click on the Finish button. Only eligible ports are displayed in the list and only one port per link is supported.

To configure a main radio, you must choose a port in an odd numbered slot.

11 Select the View the newly created Port Termination check box if you need to view the MW link member properties, and click on the Close button.

12 To configure a spare radio, right-click on the MW link where you created the main radio, and choose Create MW Link Spare Radio. Repeat steps 8 to 11.

To configure a spare radio, you must choose a port in an even numbered slot.

13 Click on the Radio tab. The tab displays information about MPT hardware and the software state of the connected radio.

14 Associate the MW link with an L2/L3 access interface or a network interface, if required.

i If you set the MW Link Member port Mode to Access in step 4, you can associate the MW link with a service, if required.

The MW links can be used in the L2 Access Interfaces of the following service types:

- VLL Epipe (see Procedure 67-27)
- VLL Ipipe (see Procedure 67-27)
- VPLS (see Procedure 68-24)
- MVPLS (see Procedure 68-24)

The MW links can also be used in the L3 Access Interfaces of the following service types:

- VPRN (see Procedure 71-22)
- IES (see Procedure 70-17)

The created access interface appears in the list on the L2 Access Interface or L3 Access Interface tab of the MW Link (Edit) form, as appropriate.

See the specific service chapter and forms when you create the required L2 or L3 access interfaces. Specify the MW Link Member as the Terminating Port.

ii If you set the MW Link Member port Mode setting to Network in step 4, the Network Interface tab is displayed. Click on the tab and then the Create button to create a network interface. The network interface that you create appears in the list. See Procedure 22-9 for more information.

15 Click on the Statistics tab to view radio analog statistical information, if required.

16 Click on the Faults tab to view alarm information, if required.

17 Click on the OK button. A dialog box appears.

18 Click on the Yes button. The MW Link Member (Edit) form closes.

Procedure 15-13 To configure 7705 SAR auxiliary alarm definitions

Perform this procedure to configure auxiliary alarm definitions for the auxiliary alarms daughter card on a 7705 SAR.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the shelf object on which you want to configure auxiliary alarm definitions. The path is Network→*NE*→Shelf.

3 Right-click on the Shelf object and choose Properties. The Shelf (Edit) form opens with the General tab displayed.

4 Click on the External Alarms tab.

5 As required, configure auxiliary alarm digital inputs.

i Click on the Auxiliary Alarm Digital Inputs tab.

ii Select a digital input from the list and click on the Properties button. The Auxiliary Alarm Digital (Edit) form opens with the General tab displayed.

iii Configure the parameters:

- Optional Name
- Description
- Administrative State
- Detection (s)
- Clearing (s)
- State

iv Click on the OK button. The Auxiliary Alarm Digital (Edit) form closes.

v Repeat steps i to iv to configure more auxiliary alarm digital inputs, as required.

6 As required, configure auxiliary alarm port inputs.

i Click on the Auxiliary Alarm Port Inputs tab.

ii Click on the Create button. The Auxiliary Alarm Ports (Create) form opens.

iii Click on the Select button beside the CLI Name parameter. The Select Port Reference - Auxiliary Alarm Ports form opens.

iv Choose a port reference from the list and click on the OK button. The Select Port Reference - Auxiliary Alarm Ports form closes.

Only Ethernet ports can be selected.

v Configure the parameters:

- Port Name
  The Port Name parameter value is automatically configured when you configure the CLI Name parameter in step iii.
- Optional Name
- Description
- Administrative State

vi Click on the OK button. A dialog box appears.

vii Click on the OK button. The Auxiliary Alarm Ports (Create) form closes.

viii Repeat steps i to vii to configure more auxiliary alarm port inputs, as required.

7 Click on the Auxiliary Alarm Definitions tab on the Shelf (Edit) form.

8 Click on the Create button. The Auxiliary Alarm Definition (Create) form opens.

9 Configure the following parameters:

- Image Files Directory
- Auto-Assign ID
- Description
- Administrative State
- Severity

10 Click on the Inputs tab and configure the following parameters:

- Trigger Rule
- Analog Threshold (mV)
- Operation
- Input 1 through Input 8 (as required)

11 Click on the Outputs tab and configure the following parameters:

- Log Event
- Update Chassis Relays

12 Click on the OK button in the Auxiliary Alarm Definition (Create) form. A dialog box appears.

13 Click on the OK button to save the configuration.

Procedure 15-14 To configure the IEEE 1588 PTP clock on a 7210 SAS, 7450 ESS, or 7750 SR

Perform this procedure to configure the IEEE 1588 PTP clock on one of the following devices that is configured as an IEEE 1588 PTP client:

- 7210 SAS-D 6F 4T ETR
- 7210 SAS-M, Release 5.0 R2 or later
- 7210 SAS-X Release 5.0 R3 or later
- Release 9.0 R4 or later 7450 ESS-7
- Release 9.0 R4 or later 7450 ESS-12
- Release 9.0 R4 or later 7750 SR-7
- Release 9.0 R4 or later 7750 SR-12
- Release 9.0 R4 or later 7750 SR-c4

See Procedure 15-7 for information about how to configure a device as a PTP client.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure the IEEE 1588 PTP clock and choose Properties. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the IEEE PTP Clock tab.

4 Select an IEEE 1588 PTP Clock from the list and click on the Properties button. The IEEE 1588 PTP Clock (Edit) form opens.

5 Configure the parameters:

- Clock Type
- Admin State
- PTP Profile
- Clock Priority 1
- Clock Priority 2
- Domain
- Network Type
- Log sync interval

At least one IEEE PTP peer must be created before you can set the Admin State parameter to Enabled. See Procedure 15-15.

When the Admin State parameter is set to Enabled, you cannot change the Clock Type, PTP Profile, Domain or Log sync interval parameters.

For the 7210 SAS-D 6F 4T ETR, 7210 SAS-M, and 7210 SAS-X, when the Clock Type parameter is set to Boundary, you must set the PTP Profile parameter to IEEE-1588-2008.

6 Click on the OK button. The IEEE 1588 PTP Clock (Edit) form closes.

7 Click on the OK button to save the configuration and close the Network Element (Edit) form.

Procedure 15-15 To configure the IEEE 1588 PTP peer of a 7210 SAS, 7450 ESS, or 7750 SR

Perform this procedure to configure the IEEE 1588 PTP peer of one of the following devices that has the IEEE 1588 PTP clock configured:

- 7210 SAS-D 6F 4T ETR
- 7210 SAS-M, Release 5.0 R2 or later
- 7210 SAS-X Release 5.0 R3 or later
- Release 9.0 R4 or later 7450 ESS-7
- Release 9.0 R4 or later 7450 ESS-12
- Release 9.0 R4 or later 7750 SR-7
- Release 9.0 R4 or later 7750 SR-12
- Release 9.0 R4 or later 7750 SR-c4

See Procedure 15-14 for information about how to configure the IEEE 1588 PTP clock on a device.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure the IEEE 1588 PTP clock and choose Properties. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the IEEE PTP Clock tab.

4 Choose an entry in the list and click on the Properties button. The IEEE 1588 PTP Clock (Edit) form opens.

5 Click on the IEEE PTP Peers tab.

6 Perform one of the following:

a To create an IEEE 1588 PTP peer on a slave, go to step 7.

b To modify an existing IEEE 1588 PTP peer on a slave, go to step 10.

7 Click on the Create button. The IEEE 1588 PTP Peer (Create) form opens

8 Configure the parameters:

- Peer ID
- Peer IP Address
- Peer Priority
- Administrative State

9 Go to step 12.

10 Select an IEEE 1588 PTP peer from the list and click on the Properties button. The IEEE 1588 PTP Peer (Edit) form opens.

11 Configure the parameters:

- Peer Priority
- Administrative State

12 Click on the OK button. The IEEE 1588 PTP Peer (Create) form closes and a dialog box appears.

13 Click on the OK button. The IEEE 1588 PTP Clock (Edit) form reappears with the IEEE 1588 PTP Peer information displayed.

14 Click on the OK button. The Network Element (Edit) form reappears.

15 Click on the OK button. A dialog box appears.

16 Click on the OK button to save the configuration and close the Network Element (Edit) form.

Procedure 15-16 To manage an OmniSwitch running configuration



Caution — When you reboot an OmniSwitch that is in service it is service-affecting. Ensure that the reboot activity occurs during a maintenance window.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the OmniSwitch object.

3 Right-click on a device and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 Click on a shelf object. The Shelf (Edit) form opens with the General tab displayed.

5 Click on the Software Control Module tab.

6 Configure the Command to Apply parameter.

a If you specify Copy certified to working, configure the Active Timeout parameter.

b If you specify Reload from working, configure the Delayed Activation Timer parameter.

7 Click on the OK button. The Shelf (Edit) form closes.

Procedure 15-17 To configure OmniSwitch health monitoring

The health monitoring function monitors the consumable resources, such as bandwidth and CPU usage of the OmniSwitch at fixed intervals and collects the current values for each resource being monitored. You can specify the resource threshold limits. If a resource value is greater or less than the threshold, traps are sent to the 5620 SAM.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the OmniSwitch NE object.

3 Right-click on the OmniSwitch device for which you need to configure health monitoring and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 Click on a shelf object. The Shelf (Edit) form opens with the General tab displayed.

5 Click on the Health Monitoring tab.

6 Configure the following parameters:

- Rx Threshold (%)
- TxRx Threshold (%)
- Temperature Threshold Unit
- Temperature Threshold
- Memory Threshold (%)
- CPU Threshold (%)
- Sampling Interval (seconds)

7 Click on the Statistics tab and search for Card Health Stats (Physical Equipment) or Device Health Stats (Physical Equipment) to view card statistics or chassis statistics respectively. Statistics can also be viewed from the card-level statistics tab.

8 Click on the Faults tab to view alarm information.

9 Click on the OK button. A dialog box appears.

10 Click on the Yes button. The Shelf (Edit) form closes.

Procedure 15-18 To configure a CCM on a 7950 XRS-20

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the 7950 XRS-20 device where you want to view CCM properties and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf object.

4 Right-click on a CCM object and choose Properties from the contextual menu. The CCM (Edit) form opens with the General tab displayed.

5 Click on the tabs to view CCM properties, as required.

6 If required, perform the following steps to configure a flash memory module.

i Click on the Flash Memory Modules tab.

ii Select a flash memory module in the list and click on the Properties button. The Flash Memory (Edit) form opens with the General tab displayed.

iii Configure the Administrative State parameter.

iv Click on the OK button. The Flash Memory (Edit) form closes.

7 If required, click on the View CPM button to open the properties form of the associated CPM.

See Procedure 15-32 for more information about the CPM properties form.

8 Click on the OK button. The CCM (Edit) form closes.

9 Close the Network Element (Edit) form.

Procedure 15-19 To manage the internal fan on a 7210 SAS-D

Perform this procedure to change the administration mode and view the fan operational state for the 7210 SAS-D 128 Mbyte variant, Release 5.0 R2 or later.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the Fan Tray object. The path is NE→Shelf→Fans→Fan Tray.

3 Right-click on Fan Tray and choose Properties from the contextual menu. The Fan Tray (Edit) form opens with the General tab displayed.

4 Click on the Fans tab. A list form opens.

5 Choose a fan from the list. The Fan (Edit) form opens with the General tab displayed.

6 Configure the Admin Mode parameter. The operational state of the fan (On or Off) is displayed in the Oper Mode field.

7 Close the Fan (Edit) form.

8 Close the Fan Tray (Edit) form.

Procedure 15-20 To configure a power supply tray

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the power supply tray object. The path is NE→Shelf→Power Supplies→Power Supply Tray.

3 Right-click on power supply tray and choose Properties from the contextual menu. The Power Supply Tray (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- Current OLC State
- Revert OLC State

5 Click on the OK button. The Power Supply Tray (Edit) form closes.

Procedure 15-21 To configure a power management zone

Use this procedure to configure a power management zone on a 7950 XRS node

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the 7950 XRS and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Power Management Zones tab. A list of power management zones is displayed.

4 Select a power management zone from the list and click on the Properties button. The Power Management Zone (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Management Mode
- Power Safety Level (%)
- Power Safety Alert (Watts)
- Overload On Power Shortage

6 Click on the Power Utilization and Power Requirements tabs to view information about power usage in the power management zone. Click on the ellipsis button (...) for detailed information about each entry.

7 Click on the OK button. The Power Management Zone (Edit) form closes.

8 Close the Network Element (edit) form.

Procedure 15-22 To provision a PEQ on a 7950 XRS

Use this procedure to provision PEQ and APEQ objects on 7950 XRS nodes.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the Power Supplies tray object. The path is NE→Shelf→Power Supplies→Power Supply Tray.

3 Right-click on a power supply tray and choose Configure PEQ. The Power Supply Tray form appears.

4 Configure the parameters:

- Assigned PEQ Type
- Current OLC State
- Revert OLC State

5 Click on the OK button. The Power Supply Tray form closes, and the Equipment navigation tree is updated with the provisioned PEQ.

15.8 Card and card slot object configuration procedures

Use the following procedures to configure card and card slot objects using the navigation tree.

Procedure 15-23 To assign a card type

Perform this procedure to assign a card type to an empty card slot or SFM slot.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to assign a card type and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf object.

4 Right-click on an empty Card Slot object or SFM Slot object and choose Configure Card from the contextual menu. The Card Slot (Create) or SFM Slot (Create) form opens.

5 Configure the parameters:

- Capability
- Assigned Card Type
- Shutdown IOM for Memory Parity Errors

Note — The correct chassis mode must be configured for the assigned card types. The chassis mode determines the behavior of the card and establishes the scaling limits and available features. See Procedure 15-1and 15-6 for more information.

6 Configure the following parameters in the Virtual Scheduler panel, if applicable:

- Fast Queue (%)
- Slow Queue (%)
- Schedule Minimum Interval (%)
- Task Scheduling Interval (%)
- Slow Queue Rate Threshold (kbps)

7 Configure the following parameters in the OLC panel:

- Current OLC State
- Revert OLC State

8 Click on the OK button. The Card Slot (Create) or SFM Slot (Create) form closes.

The card and slot appear in the navigation tree and in the equipment inventory list.

Procedure 15-24 To configure egress WRED queue control on an XCM, IOM 3 or IMM forwarding plane

Perform this procedure to configure the egress WRED queue control function on an XCM,IOM 3 or IMM.

Note — You cannot configure a forwarding plane on an XCM card until you have provisioned the corresponding XMA card.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the card slot object on which you want to configure egress WRED queue control on an IOM 3 or IMM forwarding plane. The path is Network→*NE*→Shelf→Card Slot *n*.

3 Right-click on the Card Slot object and choose Properties. The Card Slot (Edit) form opens with the General tab displayed.

4 Click on the Forwarding Plane tab.

5 Choose an entry in the list and click on the Properties button. The Forwarding Plane (Edit) form opens with the General tab displayed.

6 Configure the Egress WRED Queue Control parameters:

- Administrative State
- Buffer Allocation Min (%)
- Buffer Allocation Max (%)
- Reserved CBS Min (%)
- Reserved CBS Max (%)

7 Click on the Select button in the Slope Policy panel. The Select Slope Policy - Forwarding Plane form opens.

8 Choose a policy in the list and click on the OK button. The Select Slope Policy - Forwarding Plane form closes, and the slope policy name is displayed in the Slope Policy panel.

9 Click on the OK button. The Forwarding Plane (Edit) form closes.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The Card Slot (Edit) form closes.

Procedure 15-25 To configure IMPM on an XCM, 2 x XP MDA IOM 3, or IMM forwarding plane

Perform this procedure to configure IMPM on an XCM, 2 x XP MDA IOM 3, or an IMM.



Note 1 — See Procedure 15-34 for information about configuring IMPM on an MDA that is not installed in an XCM, 2 × XP MDA IOM 3, or in an IMM.

Note 2 — You cannot configure a forwarding plane on an XCM card until you have provisioned the corresponding XMA card.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the card slot object on which you want to configure IMPM. The path is Network→*NE*→Shelf→Card Slot *n*.

3 Right-click on the Card Slot object and choose Properties. The Card Slot (Edit) form opens with the General tab displayed.

4 Click on the Forwarding Plane tab.

5 Choose an entry in the list and click on the Properties button. The Forwarding Plane (Edit) form opens.

6 Click on the Clear button to remove the selected policy. The Select button in the BW Policy panel is enabled.

7 Click on the Select button in the BW Policy panel. The Select BW Policy form opens.

8 Choose a policy in the list and click on the OK button. The Select BW Policy form closes, and the policy name is displayed in the BW Policy panel.

9 Configure the Administrative State parameter.

10 Configure the following parameters:

- High Bandwidth Source
- High Bandwidth Multicast Traffic Taps Group
- High Bandwidth Alarm
- High Bandwidth Default Paths Only

11 Click on the OK button. The Forwarding Plane (Edit) form closes.

12 Click on the OK button. A dialog box appears.

13 Click on the Yes button. The Card Slot (Edit) form closes.

Procedure 15-26 To configure an ingress queue group on a forwarding plane



Note 1 — You can configure ingress queue groups only on the forwarding planes of XCM, IOM3, and IMM cards.

Note 2 — You cannot configure a forwarding plane on an XCM card until you have provisioned the corresponding XMA card.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the card slot object on which you want to configure ingress queue groups. The path is Network→*NE*→Shelf→Card Slot *n*.

3 Right-click the Card Slot object and choose Properties. The Card Slot (Edit) form opens with the General tab displayed.

4 Click the Forwarding Plane tab.

5 Choose an entry in the list and click the Properties button. The Forwarding Plane (Edit) form opens with the General tab displayed.

6 Perform one of the following:

a Click the Access Ingress Queue Group tab.

b Click the Network Ingress Queue Group tab.

7 Click the Create button. The Forwarding Plane Ingress Queue Group (Create) form opens with the General tab displayed.

8 Click the Select button in the Queue Group Instance panel. The Select Queue Group Template Policy form opens.

9 Choose an ingress queue group template policy from the list and click the OK button. The Select Queue Group Template Policy form closes.



Note — If you select a policy that contains queues, a configuration error message will appear when you try to apply the changes.

10 Configure the Instance ID parameter.

11 Configure the Description parameter.

12 Click the Select button beside the ID parameter in the Accounting Policy panel. The Select Accounting Policy list form opens.

13 Choose an accounting policy from the list and click the OK button. The Select Accounting Policy list form closes and the Forwarding Plane Ingress Queue Group (Create) form refreshes with the accounting policy information.



Note 1 — Only accounting policies with Queue Group Packets as record type are supported.

Note 2 — You can also choose to create an accounting policy from this form by clicking the Create button instead of the Search button. Refer to Procedure 76-7 for information on creating an accounting policy and the *5620 SAM Statistics Management Guide* for general information about configuring and collecting accounting statistics.

14 Configure the Collect Accounting Statistics parameter.

15 Click the Select button in the Policer Control Policy panel to assign a policer policy to the card. The Select Policer Control Policy form opens.

16 Choose a policer policy from the list and click the OK button. The Select Policer Control Policy form closes.

17 Click the Create button in the Ingress Policer Control Override panel. The Ingress Policer Control Override (Create) form opens, with the General tab displayed.

18 Configure the parameters:

- Maximum Frame Based Bandwidth (kbps)
- Minimum Separation Buffer Space (bytes)

19 A message is displayed. Click OK.

20 Click the Level Override Policy Items tab.

21 Select an item from the list and click OK. The FP Ingress Policer Level Override form opens, with the General tab displayed.

22 Click the Override tab.

23 Configure the Maximum Cumulative Buffer Space (bytes) parameter.

24 Click OK. The FP Ingress Policer Level Override form closes.

25 Click OK. The Ingress Policer Control Override (Create) form closes.

26 Click the Override Policy Items tab.

27 Click the Create button. The Forwarding Plane Ingress Queue Group Policer Override (Create) form opens.

28 Click the Select button beside the ID parameter to select a policer. The Select Ingress Queue Group Policer form opens.

29 Choose an entry from the list and click the OK button. The Select Ingress Queue Group Policer closes and the Forwarding Plane Ingress Queue Group Policer Override (Create) form refreshes with the policer information.

30 Click the Override tab.

31 Configure the parameters in the Overridden Queue Group Template Policer panel:

- Override PIR
- Override CIR
- Override Maximum Burst Size
- Override Committed Burst Size
- Override Packet Offset
- Stats Mode

The parameters are configurable when the associated override check box is enabled.

32 Click the OK button to save the configuration and close the Forwarding Plane Ingress Queue Group Policer Override (Create) form. A dialog box appears.

33 Click the OK button.

34 Click the OK button. The Forwarding Plane Ingress Queue Group (Create) form closes and the list in the Forwarding Plane (Edit) form is refreshed.

35 To add another access ingress or network ingress queue group, repeat steps 6 to 34. Otherwise, continue to step 36.

36 Click the OK button. A dialog box appears.

37 Click the Yes button to save the configuration and close the Forwarding Plane (Edit) form.

38 Close the Network Element (Edit) form.

Procedure 15-27 To configure NE DDoS protection on a forwarding plane

Perform this procedure to configure the maximum number of enforcement policers for a DDoS protection configuration on a forwarding plane. See “DDoS protection” in the *5620 SAM System Administrator Guide* for more information.



Note — You cannot configure a forwarding plane on an XCM card until you have provisioned the corresponding XMA card.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the card slot object on which you want to configure ingress queue groups. The path is Network→*NE*→Shelf→Card Slot *n*.

3 Right-click on the Card Slot object and choose Properties. The Card Slot form opens with the General tab displayed.

4 Click on the Forwarding Plane tab.

5 Choose an entry in the list and click on the Properties button. The Forwarding Plane (Edit) form opens with the General tab displayed.

6 Configure the NE DDoS Protection - Dynamic Enforcement Policer Pool Size parameter. Select the Default check box to specify a default value.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button to save the configuration and close the Forwarding Plane (Edit) form.

9 Close the Card Slot form.

Procedure 15-28 To enable named pool mode

Perform this procedure to allow named pools to be created for an MDA. Set the Pool Mode parameter when you are configuring the card. Enabling the Named Pool mode is mutually exclusive with enabling Stable Pool sizing.



Caution — The Pool Mode parameter can be enabled and disabled at anytime, however changing the pool mode resets the IOM when MDAs are provisioned on the slot. If MDAs are not provisioned the IOM is not reset.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the card slot object on which you want to enable named pool mode. The path is Network→*NE*→Shelf→Card Slot *n*.

3 Right-click on the Card Slot object and choose Properties. The Card Slot (Edit) form opens with the General tab displayed.

4 Click on the IO Card tab.

5 Configure the Pool Mode parameter.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The Card Slot (Edit) form closes.

Procedure 15-29 To enable Stable Pool Sizing

Perform this procedure to enable an even split of buffering amongst all possible MDAs.

When Stable Pool sizing is enabled, then for each MDA, the buffering is split between all ports based on the port maximum bandwidth and adjusted by the port's modify buffer allocation rate percentages. You cannot enable Stable Pool Sizing on any forwarding plane on a card while the card is either administratively or operationally in Named Pool mode.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the card slot object on which you want to enable Stable Pool sizing. The path is Equipment→*NE*→Shelf *n*→Card Slot *n*.

3 Right-click on the Card Slot object and choose Properties. The Card Slot (Edit) form opens with the General tab displayed.

4 Click on the Forwarding Plane tab.

5 Select the required forwarding plane from the list and click Properties. The Forwarding Plane (Edit) form opens.

6 Configure the Stable Pool Sizing parameter.

7 Click on the OK button. The Forwarding Plane (Edit) form closes.

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button. The Card Slot (Edit) form closes.

Procedure 15-30 To configure OmniSwitch stacks

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on an OmniSwitch object and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf object.

4 Click on a slot object. The Card Slot (Edit) form opens with the General tab displayed.

5 Click on the Stack Configuration tab.

6 Configure the parameters, as applicable to a given OmniSwitch NE:

- Saved Slot NI Number
- Command Action
- Stacking Action
- Administrative
- Operational

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The Card Slot (Edit) form closes.

Procedure 15-31 To configure an OmniSwitch CPU temperature threshold

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on an OmniSwitch object and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf object.

4 Click on a slot object. The Card Slot (Edit) form opens with the General tab displayed.

5 Click on the Hardware Environment tab.

6 Configure the Temperature Threshold (Celsius) parameter.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The Card Slot (Edit) form closes.

Procedure 15-32 To configure a CPM on a 7950 XRS

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the 7950 XRS device where you want to view CPM properties and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf object.

4 Right-click on Card Slot A or Card Slot B and choose Properties from the contextual menu. The Card Slot (Edit) form opens with the General tab displayed.



Note — Card Slot A and Card Slot B are automatically configured with CPMs. The CPMs cannot be removed, and they cannot be configured in any other card slot.

5 Configure the parameters:

- Current OLC State
- Revert OLC State

6 Click on the tabs to view CPM properties, as required.

7 If you are configuring a CPM on a 7950 XRS-16c, the Flash Memory Modules tab is available. If required, perform the following steps to configure a flash memory module on a 7950 XRS-16c.

i Click on the Flash Memory Modules tab.

ii Select a flash memory module in the list and click on the Properties button. The Flash Memory (Edit) form opens with the General tab displayed.

iii Configure the Administrative State parameter.

iv Click on the OK button. The Flash Memory (Edit) form closes.



Note — You can configure flash memory modules on the 7950 XRS-20 from the CCM properties form. See Procedure 15-18 for more information.

8 If you are configuring a CPM on a 7950 XRS-20, the View CCM button is available. If required, click on the View CCM button to open the properties form of the associated CCM.

See Procedure 15-18 for more information about the CCM properties form.

9 Click on the OK button. A dialog box appears.

10 Click on the OK button. The Card Slot (Edit) form closes.

11 Close the Network Element (Edit) form.

15.9 Daughter card slot object configuration procedures

Use the following procedures to configure daughter card slot objects using the navigation tree.

Procedure 15-33 To configure an MDA

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure an MDA and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf object and the Card Slot object.

4 Perform one of the following.

a To add a daughter card to an empty daughter card slot, right-click on the daughter card slot and choose Configure Daughter Card from the contextual menu. The Daughter Card Slot (Create) form opens.

b To modify an existing daughter card, click on the daughter card slot. The Daughter Card Slot (Edit) form opens.



Note — If a daughter card in your configuration is managed by 5620 SAM but becomes no longer supported by 5620 SAM (for instance, an obsoleted MDA), it will be displayed under the equipment tree as type Unspecified. To delete such a card from 5620 SAM, you must remove the MDA from the device. Once a card is removed from the device, it is also automatically deleted from 5620 SAM.

5 Configure the parameters, if applicable:

- Assigned Daughter Card Type
- In MDA Carrier Module Slot
- Clock Mode
  The Clock Mode parameter value must be set to Differential in order to configure the Differential Timestamp Frequency (kHz) parameter.
- Differential Timestamp Frequency (kHz)
- Current OLC State
- Revert OLC State
- ATM Mode



Note 1 — The Assigned Daughter Card Type and In MDA Carrier Module Slot parameters are configurable only during daughter-card creation.

Note 2 — The Clock Mode and Differential Timestamp Frequency (kHz) parameters are configurable on a 16/32 × Channelized DS1/E1 ASAP v2 in a Release 6.0 R1 or later 7705 SAR-8, 7705 SAR-8 v2, or 7705 SAR-18, a 4 × Channelized DS3/E3 ASAP in a Release 6.0 R3 or later 7705 SAR, and an ASAP channelized card in a Release 6.0 R2 or later 7705 SAR-A. Combo MDA is supported on the 7705 SAR-H.

Note 3 — The ATM Mode parameter can only be configured on an MDA card of type 4 × ATM OC3/OC12, 4 × ATM OC3 STM1, or 16 port ATM OC3 STM1 on 7750 SR cards (excluding 7750 SR-c4 and 7750 SR-c12) on an IOM 3 card.

Note 4 — The ATM Mode parameter must be set to a value of max16k-vc for PPPoA and PPPoEoA to be supported.

6 If you are creating a daughter card on a 7710 SR, perform the following steps.

i Click on the MDA Carrier Module tab.

ii Configure the Assigned MCM Card Type parameter.

7 Click on the Apply button.

8 Click on the Daughter Card tab.

9 Configure the parameters:

- Administrative State
- MDA Mode
- Synchronous Ethernet
- Fabric Stats
- Power Priority Level



Note 1 — The MDA Mode parameter can only be configured on 16 x Channelized DS1/E1 ASAP v2, 32 x Channelized DS1/E1 ASAP v2, 4 x Channelized DS1/E1 ASAP, or XMDA 1p x 10GigE / 10p x 1GigE SFP.

Note 2 — Before you configure the MDA Mode parameter, you must shut down all of the ports and remove all of the subchannels and bundles from the MDA.

10 Configure the following parameters in the Voice panel, if required:

- Companding Law
- Signalling Type

11 Perform the following steps to configure named buffer pools, if required.



Note — You must enable pool mode on the parent I/O card to enable named buffer pool support. See Procedure 15-28 for more information.

i Click on the Select button beside the Name parameter in the Ingress Pool Policy panel. The Select Ingress Pool Policy form opens.

ii Choose a policy in the list and click on the OK button. The Select Ingress Pool Policy form closes, and the policy name is displayed in the Ingress Pool Policy panel.

iii If you are configuring an HSMDA daughter card, go to step 13.



Note — HSMDA daughter cards support only ingress named buffer pool policies, and not egress named buffer pool policies.

iv Click on the Select button beside the Name parameter in the Egress Pool Policy panel. The Select Egress Pool Policy form opens.

v Choose a policy in the list and click on the OK button. The Select Egress Pool Policy form closes, and the policy name is displayed in the Egress Pool Policy panel.

12 Perform the following steps to assign a network queue policy, if required.

i Click on the Select button in the Network Queue Policy panel. The Select Network Queue Policy form opens.

ii Select a policy in the list and click on the OK button. The Select Network Queue Policy form closes, and the policy is displayed in the Network Queue Policy panel.

13 Perform the following steps to configure HSMDA pool policies, if required.



Note — You must enable pool mode on the parent I/O card to enable HSMDA pool support. See Procedure 15-28 for more information.

i Click on the Select button in the Egress HSMDA Pool Policy panel. The Select Egress HSMDA Pool Policy form opens.

ii Choose a policy in the list and click on the OK button. The Select Egress HSMDA Pool Policy form closes, and the policy is displayed in the Egress HSMDA Pool Policy panel.

14 Configure the following parameters in the HSMDA Aggregate Queue Burst panel, if required:

- Threshold Low Burst Multiplier
- Threshold High Burst Increase

15 Perform the following steps to add a fabric profile, if required.

i Click on the Select button in the Network Ingress Fabric Profile panel. The Select Fabric Profile form opens.

ii Choose a profile in the list and click on the OK button. The Select Network Ingress Fabric Profile form closes, and the profile name is displayed in the Network Ingress Fabric Profile panel.

iii Click on the Select button in the Access Ingress Fabric Profile panel. The Select Fabric Profile form opens.

iv Choose a profile in the list and click on the OK button. The Select Access Ingress Fabric Profile form closes, and the profile name is displayed in the Access Ingress Fabric Profile panel.

16 Perform the following steps to assign a network queue policy and network policy of ring type for a 7705 SAR, if required.

i Click on the Select button in the Ring Policies panel. The Select Network Queue Policy form opens.

ii Choose a network queue policy in the list and click on the OK button. The Select Network Queue Policy closes, and the policy is displayed in the Ring Policies panel.

iii Click on the Select button in the Network Policy panel. The Select Network Policy form opens.

iv Choose a network policy in the list and click on the OK button. The Select Network Policy form closes and the policy is displayed in the Network Policy panel.



Note — To assign a network policy of ring type to a 7705 SAR-8 or 7705 SAR-18 MDA, you must set the Network Policy Type for 7705 parameter to Ring when you configure a network policy on the MDA. See Procedure 43-6 for more information.

17 Perform the following steps to configure MAC management, if required.

i Click on the MAC Operation tab. The FDB Mac Management tab appears.

ii Configure the parameters, if applicable:

- Mac Learning
- Mac Aging
- Discard Unknown Source
- Remote Age (seconds)
- Forwarding DB Size (entries)
- Mac Pinning on Port 1
- Mac Pinning on Port 2
- Fdb Table High Watermark

iii To create an FDB Mac entry, click on the FDB Entries tab. The MDA MAC FDB Management (Create) form opens.

iv Configure the parameters:

- Mac Address
- Name

v Click on the Select button in the Port panel. The Select Port - MDA MAC FDB Management form opens.

vi Choose a port in the list and click on the OK button. The Select Port - MDA MAC FDB Management form closes, and the port is displayed in the Port panel of the MDA MAC FDB Management form.



Note — You can only bind a ring port to an FDB Mac entry.

vii Click on the OK button. The FDB Mac entry is displayed in the FDB Entries form.

18 Click on the Network Interfaces tab to add a network interface card, if required.

19 Click on the Add button. The Create Network Interface - Routing Instance form opens. Perform steps 4 to 49 of Procedure 22-9 to create a network interface.

20 Perform steps 2 to 5 of Procedure 15-34 to configure IMPM on the daughter card, if required.

21 If you configured named buffer pools in step 11, perform the following steps to configure the associated Q1 pools. Otherwise, go to step 22.



Note — You cannot use this step to configure 7710 SR QoS policies.

i Click on the QoS Pool tab.

ii Choose a pool in the list and click on the Properties button. The QoS Pool (Edit) form opens.

iii Configure the parameters:

- Reserved CBS (%)
- Default Reserved CBS
- Amber Alarm Action Max (%)
- Amber Alarm Action Step (%)
- Amber Alarm Threshold (%)
- Red Alarm Threshold (%)

iv Click on the Select button in the Slope Policy panel. The Select Slope Policy - QoS Pool form opens.

v Choose a policy in the list and click on the OK button. The Select Slope Policy - QoS Pool form closes, and the slope policy name is displayed in the Slope Policy panel.

22 Perform the following steps to configure ATM, if required.

i Click on the ATM tab.

ii Select an ATM configuration from the list and click on the Properties button. The ATM Configuration (Edit) form opens.

iii Click on the VP Shaping tab.

iv Click on the Create button. The ATM VP Shaper (Create) form opens.

v Configure the VP ID parameter.

vi Click on the Select button in the ATM QoS Policy panel. The Select ATM QoS Policy - ATM VP Shaper form opens.

vii Select an ATM QoS Policy from the list and click on the Properties button. The ATM QoS Policy (Edit) form opens.

viii Click on the QoS tab.

ix Configure the VP Shaping Weight parameter.

x Click on the OK button. A dialog box appears.

xi Click on the Yes button. The ATM QoS Policy (Edit) form closes.

xii Click on the OK button. The Select ATM QoS Policy - ATM VP Shaper form closes.

xiii Click on the OK button. A dialog box appears.

xiv Click on the OK button. The ATM VP Shaper (Create) form closes.

xv Repeat steps iv to xiv to create additional ATM VP shapers, if required.

xvi Click on the OK button. A dialog box appears.

xvii Click on the Yes button. The ATM Configuration (Edit) form closes.

23 Click on the OK button. A dialog box appears.

If you are adding a new daughter card, the daughter card and the contained ports are displayed in the navigation tree.

24 Click on the Yes button. The Daughter Card Slot properties form closes.

Procedure 15-34 To configure IMPM on an MDA

Perform this procedure to configure IMPM on an MDA that is not installed in an XCM, 2 x XP MDA IOM 3 or an IMM.



Note — See Procedure 15-25 for information about configuring IMPM on an XCM, 2 × XP MDA IOM 3 or IMM.

1 Perform steps 1 to 8 of Procedure 15-33.

2 Configure the following parameters in the Daughter Card Details panel:

- High Bandwidth Source
- High Bandwidth Multicast Traffic Taps Group
- High Bandwidth Alarm

3 Click on the Select button in the BW policy panel to choose a multicast bandwidth policy. The Select BW Policy form opens.

4 Choose a policy in the list and click on the OK button. The Select BW Policy form closes and the policy name is displayed in the BW Policy panel.



Note — The multicast bandwidth policy named “default” cannot be modified or deleted.

5 Configure the following parameters in the Multicast Path Management panel:

- Administrative State
- Primary Path Limit (mbps)
- Secondary Path Limit (mbps)
- Ancillary Path Limit (mbps)

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The Daughter Card Slot properties form closes.

Procedure 15-35 To view the operational multicast channel properties of an MDA

Perform this procedure to view specific information about an operational multicast channel on an MDA that is configured to use an Ingress Multicast Bandwidth policy.



Note — You can also view operational multicast channel information in the following locations:

- the Mcast Path Mgmt tab on the properties form of a VPLS or VPRN service site
- the Mcast Path Mgmt Channels tab on the properties form of a routing instance.

Each properties form contains information about the ingress MDA of each operational channel.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to view operational multicast channel properties on an MDA and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf object.

4 Expand the Card Slot object. The Card Slot (Create) form opens with the General tab displayed.

5 Click on the daughter card slot object. The Daughter Card Slot (Edit) form opens with the General tab displayed.

6 Click on the Mcast Path Mgmt Channels tab.

7 Click on the Search button. A list of operational channels is displayed.

8 View the information, which includes the service site or routing instance associated with the channel, and the following properties:



Note — Channel information is displayed only when the MDA receives multicast traffic for a previously configured multicast group.

- Group Address—the operational channel multicast group address
- Source Address—the operational channel multicast source address
- Bandwidth—the operational bandwidth of the channel
- Administrative Bandwidth—the administrative bandwidth of the channel
- Last Highest Bandwidth—the value of the multicast bandwidth that is currently allocated to the channel forwarding path on the MDA. This value is calculated based on periodic statistics polls and represents the highest recorded bandwidth value since the most recent restart of the bandwidth update timer for the channel.
- Second Highest Bandwidth—the second-highest recorded bandwidth value for the channel since the most recent restart of the bandwidth update timer. The value is calculated based on periodic statistics polls and is reset to zero every time the bandwidth update timer for the channel is restarted.
- BW Update Timer expiration—the time that remains before the bandwidth update timer for the channel expires
- Current Path—the path that the channel traffic uses to reach the switching fabric; the path value is primary, secondary, or ancillary
- Explicit Path—indicates whether the current path is explicitly specified by a Multicast Info Policy
- Preference Level—the preference level of the channel
- Black-Hole—whether the channel is in the Black-Hole state
- Black-Hole Rate—specifies the bandwidth rate, in kb/s, at which the channel enters the Black-Hole state

9 Close the Daughter Card Slot (Edit) form.

Procedure 15-36 To configure a 7705 SAR module card

Perform this procedure to configure a module card on a 7705 SAR-M or 7705 SAR-ME.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the 7705 SAR-M/ME device on which you need to configure an MDA and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf object and the Card Slot object.

4 Right-click on the third Daughter Card Slot object and choose Configure Daughter Card from the contextual menu. The Daughter Card Slot (Create) form opens with the General tab displayed.



Note — Only the third daughter card slot can be configured with module cards. The other two slots are configured with integrated cards that cannot be removed.

5 Configure the Assigned Daughter Card Type parameter.

6 Click on the Apply button. The Daughter Card Slot form refreshes.

7 Click on the Daughter Card tab.

8 Configure the parameters:

- Administrative State
- Fabric Stats

9 Add a fabric profile, if required:

i Click on the Select button in the Network Ingress Fabric Profile panel. The Select Fabric Profile form opens.

ii Choose a profile and click on the OK button. The Select Network Ingress Fabric Profile form closes and the profile name is displayed in the Network Ingress Fabric Profile panel.

iii Click on the Select button in the Access Ingress Fabric Profile panel. The Select Fabric Profile form opens.

iv Choose a profile and click on the OK button. The Select Access Ingress Fabric Profile form closes and the profile name is displayed in the Access Ingress Fabric Profile panel.

If you are configuring a 1 Colour Optical Add/Drop Mux card, go to step 25.

10 Click on the Ports tab.

11 Choose a port and click on the Properties button. The Physical Port (Edit) form opens with the General tab displayed.



Note — The first port on the DCM includes four SHDSL lines. The second port includes two XDSL lines.

12 Configure the parameters:

- Description
- Configured MAC
- Mode
- Encap Type
- Speed
- MTU (bytes)
- DDM Event Suppression
- Current OLC State

13 Click on the States tab.

14 Configure the Administrative State parameter. If you are configuring a DCM or DSL module, go to step 17.

15 Click on the GPON tab.

16 Configure the parameters and go to step 22:

- Subscriber Location ID (SLID)
- Subscriber Location ID (SLID) Format
- Dot1 Q Ethertype
- CFM LoopBack Mode
- Down When Looped
- Egress Rate (Kbps)
- Type
- Time (seconds)
- Keep Alive Interval (Sec)
- Retry Timeout (Sec)
- Use Broadcast Address

17 Click on the DSL tab.

18 Configure the parameters:

- Dot1 Q Ethertype
- CFM LoopBack Mode
- Adsl2Plus
- Down When Looped
- Egress Rate (Kbps)
- Type
- Time (seconds)
- Synchronous status messages
- SSM Code-Type
- Keep Alive Interval (Sec)
- Retry Timeout (Sec)
- Use Broadcast Address

19 Configure XDSL or SHDSL lines, if required.

i Click on the XDSL or SHDSL tab, as appropriate.

ii Choose an XDSL or SHDSL line and click on the Properties button. The XDSL Line (Edit) or SHDSL Line (Edit) form opens with the General tab displayed.

iii Configure the Administrative State parameter.

iv Click on the OK button. The XDSL Line (Edit) or SHDSL Line (Edit) form closes.

v Repeat steps i to iv to configure more lines, if required.

20 Click on the Ethernet tab.

21 Perform steps 7 to 11 of Procedure 32-42.

22 Click on the OK button. A dialog box appears.

23 Click on the Yes button. The Physical Port (Edit) form closes.

24 If you are configuring a DCM, repeat steps 11 to 23 to configure the second port.

25 Close the Daughter Card Slot (Edit) form.

15.10 Bundle configuration procedures

Use the following procedures to manage bundles using the navigation tree. You can configure bundles only on channelized MDAs.

Procedure 15-37 To create an FR group bundle

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you need to create an FR group bundle and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf object.

4 Expand the card slot object on which the channelized daughter card resides, on which you want to create the bundle.

5 Expand the channelized daughter card slot object on which you need to create the bundle.

6 Right-click on the Bundles object and choose Create Bundle from the contextual menu. The Create Multilink Bundle form opens.

7 Configure the parameters:

- Bundle ID
- Auto-Assign ID
- Description
- Administrative State

8 Click on the Next button. The Configure Bundle Parameters form opens.

9 Set the Bundle Type parameter to FR.



Note 1 — To create a PPP group bundle, perform Procedure 15-41.

Note 2 — To create an IMA group bundle, perform Procedure 15-39

10 Configure the parameters:

- Fragment Threshold (bytes)
- Red Diff Delay (milliseconds)
- Red Diff Delay Action
- Minimum Links
- Yellow Diff Delay (milliseconds)

11 Click on the Next button. The Configure Bundle Members form opens.

12 Perform one of the following:

a To create the multilink bundle without adding any members, go to step 13.

b Add DS0 channel groups to the bundle by performing the following steps.

i Click on the Create button. The Add Bundle Member series of configuration steps appears.

ii Configure the Show Only Compatible Channels parameter.

iii Click on the Next button. The Select Channels form opens.

iv Choose up to 8 channel groups from the list of channels to construct the bundle.



Note — The channel group with the lowest Port ID is chosen as the primary member for the bundle. The Encap Type of the primary member is used for all other members. When adding members to a bundle at a later time, the Encap Type must be the same as the primary member to select it as a compatible member.

13 Click on the Finish button. The Configure Bundle Members form closes and the Create Multilink Bundle form reappears.

14 Click on the Finish button to close the Create Multilink Bundle form.

Procedure 15-38 To modify an FR group bundle

Perform the following procedure to modify FR group bundle parameters, add group members, and specify a test member for FR group bundle connectivity testing.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to modify an FR group bundle and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf object.

4 Expand the card slot object on which the channelized daughter card resides, on which you want to modify the bundle.

5 Expand the channelized daughter card slot object on which you want to modify the bundle.

6 Expand the Bundles object and click on an FR group bundle object. The Multilink Bundle (Edit) form for the FR group bundle opens with the General tab displayed.

7 Configure the Description parameter.

8 Click on the Multilink Bundle tab.

9 Configure the parameters:

- Fragment Threshold (bytes)
- Red Diff Delay (milliseconds)
- Red Diff Delay Action
- Minimum Links
- Yellow Diff Delay (milliseconds)

10 Click on the States tab and configure the Administrative State parameter, if required.

11 Click on the MLFR tab.

12 Configure the parameters:

- Hello Timer
- Ack Timer
- Hello Retry Count

13 Click on the Select button beside the MCFR Ingress Qos Profile parameter. The Select MCFR Ingress Qos Profile - MultiClass Mlfr list form opens.

14 Choose a profile from the list and click on the OK button. The Select MCFR Ingress Qos Profile - MultiClass Mlfr list form closes and the Multilink Bundle (Edit) form is refreshed with the MCFR Ingress QoS Profile information.

15 Click on the Select button beside the MCFR Egress Qos Profile parameter. The Select MCFR Egress Qos Profile - MultiClass Mlfr list form opens.

16 Choose a profile from the list and click on the OK button. The Select MCFR Egress Qos Profile - MultiClass Mlfr list form closes and the Multilink Bundle (Edit) form is refreshed with the MCFR Egress QoS Profile information.

17 To add members to the FR group bundle, perform the following steps.

i Click on the Bundle Members tab.

ii Click on the Create button to add DS0 channel groups to the bundle. The Add Bundle Member series of configuration steps appears.

iii Perform step 12 b of Procedure 15-39.



Note — You can also add bundle members to the FR group bundle using the contextual menu in the navigation tree.

18 Click on the L2 Access Interfaces and L3 Access Interfaces tabs to view the interfaces that the bundle is assigned to.

19 Click on the Service Access Points tab to view SAP information.

20 Click on the Statistics tab to view statistical information.

21 Click on the Faults tab to view information about alarms.

22 Configure the FR interface, if required. Perform the following steps:

i Click on the Edit FR button. If the Edit FR button is not visible, click on the More Actions button and choose Edit FR. The FR Interface Bundle form opens with the General tab displayed.

ii Configure the parameters:

- LMI Type
- LMI Mode
- Error Threshold
- Monitored Events
- Polling Interval (seconds)
- Full Enquiry Interval

23 Click on the OK button. The FR Interface Bundle form closes.

24 Close the Multilink Bundle (Edit) form.

Procedure 15-39 To create an IMA group bundle

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to create an IMA group bundle and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf object.

4 Expand the card slot object on which the channelized daughter card resides, on which you want to create the bundle.

5 Expand the channelized daughter card slot object on which you want to create the bundle.

6 Right-click on the Bundles object and choose Create Bundle from the contextual menu. The Create Multilink Bundle form opens.

7 Configure the parameters:

- Bundle ID
- Auto-Assign ID
- Description
- Administrative State

8 Click on the Next button. The Configure Bundle Parameters form opens.

9 Set the Bundle Type parameter to IMA.



Note 1 — To create a PPP group bundle, perform Procedure 15-41.

Note 2 — To create an FR group bundle, perform Procedure 15-37

10 Configure the parameters:

- Red Diff Delay (milliseconds)
- Minimum Links
- IMA Version
- ATM Interface Cell Format
- ATM Minimum VPI Value
- Test Pattern
- Link Activation Timer
- Link Deactivation Timer
- Maximum Links

11 Click on the Next button. The Configure Bundle Members form opens.

12 Perform one of the following:

a To create the multilink bundle without adding any members, go to step 13.

b Add DS0 channel groups to the bundle by performing the following steps.

i Click on the Create button. The Add Bundle Member series of configuration steps appears.

ii Click on the Next button. The Select Channels form opens.

iii Choose up to 8 channel groups from the list of channels to construct the bundle.



Note — The channel group with the lowest Port ID is chosen as the primary member for the bundle. The Encap Type of the primary member is used for all other members. When adding members to a bundle at a later time, the Encap Type must be the same as the primary member to select it as a compatible member.

13 Click on the Finish button. The Configure Bundle Members form closes and the Create Multilink Bundle form reappears.

14 Click on the Finish button to close the Create Multilink Bundle form.

Procedure 15-40 To modify an IMA group bundle

Perform the following procedure to modify IMA group bundle parameters, add group members, and specify a test member for IMA group bundle connectivity testing.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to modify an IMA group bundle and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf object.

4 Expand the card slot object on which the channelized daughter card resides, on which you want to modify the bundle.

5 Expand the channelized daughter card slot object on which you want to modify the bundle.

6 Expand the Bundles object and click on an IMA group bundle object. The Multilink Bundle (Edit) form for the IMA group bundle opens with the General tab displayed.

7 Configure the Description parameter.

8 Click on the Multilink Bundle tab.

9 Configure the parameters:

- Red Diff Delay (milliseconds)
- Minimum Links
- IMA Version
- ATM Interface Cell Format
- ATM Minimum VPI Value
- Test Pattern
- Link Activation Timer
- Link Deactivation Timer
- Maximum Links

10 To specify the IMA member that is used to test link connectivity in the IMA group bundle, perform the following steps.

   i Click on the Select button beside the Test Member parameter. The Select Interface - Multilink Bundle form opens.

   ii Choose an interface from the list.

   iii Click on the OK button. The Select Interface - Multilink Bundle form closes and the Multilink Bundle (Edit) form refreshes with the test member information.

11 Click on the Test Pattern Start button to run the test. If the Test Pattern Start button is not visible, click on the More Actions button and choose Test Pattern Start. You can click on the Test Pattern Stop button at any time to stop the test. If there Test Pattern Stop button is not visible, click on the More Actions button and choose Test Pattern Stop. The Multilink Bundle (Edit) form refreshes with the link connectivity information.

12 Click on the States tab.

13 Configure the Administrative State parameter, if required.

14 To add members to the IMA group bundle, perform the following steps.

i Click on the Bundle Members tab.

ii Click on the Create button to add DS0 channel groups to the bundle. The Add Bundle Member series of configuration steps appears.

iii Perform step 12 b of Procedure 15-39.



Note — You can also add bundle members to the IMA group bundle using the contextual menu in the navigation tree.

15 Click on the L2 Access Interfaces and L3 Access Interfaces tabs to view the interfaces that the bundle is assigned to.

16 Click on the Service Access Points tab to view SAP information.

17 Click on the Statistics tab to view statistical information.

18 Click on the Faults tab to view information about alarms.

19 Close the Multilink Bundle (Edit) form.

Procedure 15-41 To create an MLPPP bundle

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the NE on which you want to create a MLPPP bundle and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf object.

4 Expand the card slot object on which the channelized daughter card resides, on which you want to create the bundle.

5 Expand the channelized daughter card slot object on which you want to create the bundle.

6 Right-click on the Bundles object and choose Create Bundle from the contextual menu. The Create Multilink Bundle form opens.

7 Configure the parameters:

- Bundle ID
- Auto-Assign ID
- Description
- Administrative State

8 Click on the Next button. The Configure Bundle Parameters form opens.

9 Set the Bundle Type parameter to PPP.



Note 1 — To create an FR group bundle, perform Procedure 15-37

Note 2 — To create an IMA group bundle, perform Procedure 15-39.

Note 3 — If you create an MLPPP bundle and the DS1 BER exceeds a threshold, the PPP link is automatically removed from the MLPPP bundle.

10 Configure the parameters:

- Fragment Threshold (bytes)
- Red Diff Delay (milliseconds)
- Red Diff Delay Action
- Minimum Links
- Yellow Diff Delay (milliseconds)
- Bundle MRRU (bytes)
- Short Sequence
- Link Fragmentation and Interleaving

11 Click on the Next button. The Configure Bundle Members form opens.



Note — If you want to configure this MLPPP bundle for multiclass service transmission, you must not add any bundle members. Go to step 17. See Procedure 15-44 for information about how to configure the MLPPP bundle for multiclass service transmission.

12 Click on the Create button to add DS0 channel groups to the bundle. The Add Bundle Member series of configuration steps appears.

13 Configure the Show Only Compatible Channels parameter.

14 Click on the Next button. The Select Channels form opens.

15 Select compatible channels from the list to construct the bundle. Choose up to eight channel groups from the list of channels.



Note 1 — If there are no compatible channels to choose from and you have decided that you want to edit some of the existing channels that are not compatible to be compatible, click on the Back button and disable the Show Only Compatible Channels parameter. Click on the Next button. Choose channels to edit from the list and click on the Properties button.

Note 2 — The channel group with the lowest Port ID is chosen as the primary member for the bundle. The Encap Type of the primary member is used for all other members. When adding members to a bundle at a later time, the Encap Type must be the same as the primary member to select it as a compatible member.

16 Click on the Finish button. The Configure Bundle Members form closes and the Create Multilink Bundle form reappears.

17 Click on the Finish button.

18 Click on the Close button. The Create Multilink Bundle form closes.

Procedure 15-42 To modify an MLPPP bundle

Perform the following procedure to modify multilink PPP bundle parameters, add group members, and configure MC MLPPP to allow multiple classes of services to be transmitted over the bundle.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the NE on which you want to modify a multilink PPP bundle and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf object.

4 Expand the card slot object on which the channelized daughter card resides, on which you want to modify the bundle.

5 Expand the channelized daughter card slot object on which you want to modify the bundle.

6 Expand the Bundles object and click on a multilink bundle object. The Multilink Bundle (Edit) form for the PPP bundle opens with the General tab displayed.

7 Configure the Description parameter.

8 Click on the Multilink Bundle tab.

9 Configure the parameters:

- Fragment Threshold (bytes)
- Red Diff Delay (milliseconds)
- Red Diff Delay Action
- Minimum Links
- Yellow Diff Delay (milliseconds)
- Bundle MRRU (bytes)
- Short Sequence
- Link Fragmentation and Interleaving

10 Click on the States tab.

11 Configure the Administrative State parameter, if required.

12 To add members to the multilink bundle, perform the following steps.



Note — If you want to configure this MLPPP bundle for multiclass service transmission, you must not add any bundle members. Go to step 17. See Procedure 15-44 for information about how to configure the MLPPP bundle for multiclass service transmission.

i Click on the Bundle Members tab.

ii Click on the Create button to add DS0 channel groups to the bundle. The Add Bundle Member series of configuration steps appears.

iii Perform steps 13 to 15 of Procedure 15-41.

iv Click on the Finish button. The Add Bundle Member series of configuration steps closes.



Note — You can also add bundle members to the multilink bundle using the contextual menu in the navigation tree.

13 Click on the L2 Access Interfaces and L3 Access Interfaces tabs to view the interfaces that the bundle is assigned to.

14 Click on the Service Access Points tab to view SAP information.

15 Click on the Statistics tab to view statistical information.

16 Click on the Faults tab to view information about alarms.

17 Close the Multilink Bundle (Edit) form.

Procedure 15-43 To configure an MLPPP bundle for multiclass service transmission



Note — Consider the following when you configure multiclass MLPPP.

- Multiclass MLPPP is supported only on channelized ASAP MDAs on the 7705 SAR, 7710 SR, and 7750 SR.
- You must configure multiclass MLPPP before you add bundle members to the multilink bundle.
- Multiclass MLPPP is not supported when the port is configured as network mode.
- Multiclass MLPPP is not supported when LFI is enabled.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the NE on which you want to modify a multilink PPP bundle and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf object.

4 Expand the card slot object on which the channelized daughter card resides, on which you want to modify the bundle.

5 Expand the channelized daughter card slot object on which you want to modify the bundle.

6 Expand the Bundles object and click on a multilink bundle object. The Multilink Bundle (Edit) form for the PPP bundle opens with the General tab displayed.

7 Click on the MLPPP tab.

8 Configure the parameters:

- End Point ID
- End Point Class ID
- Class Count
- Magic Number



Note — The Magic Number parameter is configurable only on 7710 SR and 7750 SR channelized ASAP MDAs.

9 Click on the Select button in the MLPPP Ingress QoS Profile or MLPPP Egress QoS Profile panel to choose an MLPPP ingress or egress QoS profile. If a profile is already selected, click on the Clear button to clear the selection and enable the Select button. The Select MLPPP Ingress QoS Profile or Select MLPPP Egress QoS Profile form opens.



Note — You can only apply QoS profiles to an MLPPP bundle if the Class Count parameter is set to 4.

10 Select a profile and click on the OK button. The Select MLPPP Ingress QoS Profile or Select MLPPP Egress QoS Profile form closes.

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button.

13 Close the Multilink Bundle (Edit) form.

Procedure 15-44 To configure an MLPPP bundle as a network interface on a channelized ASAP MDA

1 Perform Procedure 15-41 to create a MLPPP bundle on a channelized ASAP MDA.



Note — Consider the following when configuring an MLPPP as a network interface.

- LFI is not supported on MLPPP network interfaces.
- MC MLPPP is not supported on MLPPP network interfaces.
- IPv6 network interfaces are not supported.
- Up to 8 network interface members can be added to a bundle.

2 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

3 Right-click on the device where you want to configure an MLPPP bundle and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 On the Network Element (Edit) form navigation tree, expand the Shelf object.

5 Expand the Bundles object and click on the bundle created in step 1. The Multilink Bundle (Edit) form opens with the General tab displayed.

6 Click on the Bundle Members tab.

7 Click on the Search button and choose a bundle member from the list. Click on the Properties button. The Bundle Member (Edit) form opens.

8 Click on the Port tab.

9 Click on the Properties button beside the port name. The DS0 Channel Group (Edit) form opens with the General tab displayed.

10 Set the Mode parameter to Network.

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The DS0 Channel Group (Edit) form closes.

13 Close the Bundle Member (Edit) form.

14 The Multilink Bundle (Edit) form refreshes with new tabs.

15 Click on the Network Interfaces tab.

16 Click on the Create button. The Create Network Interface - Routing Instance form opens.

17 Perform steps 4 to 43 of Procedure 22-9 to create a network interface on the DS0 channel.

The port in step 6 of Procedure 22-9 is set to the DS0 channel by default. Go to step 12 of Procedure 22-9.

18 The L3 interface appears on the Network Interfaces tab. Close the Multilink Bundle (Edit) form.

16 — Port and channel object configuration

16.1 Port and channel object configuration overview *16-2*

16.2 Working with port and channel objects *16-2*

16.3 SONET and SDH sub-channel applications and structure *16-18*

16.4 Workflow to manage port objects *16-25*

16.5 Workflow to manage channel objects *16-26*

16.6 Port configuration procedures *16-27*

16.7 Channel and framing link configuration procedures *16-72*

16.1 Port and channel object configuration overview

Port objects are children of daughter card slot objects. They appear below the daughter card slot after the daughter card is configured. Channel objects are children of port objects. They appear on the navigation tree below the port object after the channel is configured.

Properties forms for port objects and channel objects are accessed using the 5620 SAM navigation tree.

This chapter contains the procedures to configure devices using the navigation tree. See chapter 5 for more information about using the navigation tree.

16.2 Working with port and channel objects

The types of ports that are available depend on the daughter cards that are configured in the chassis. For some OmniSwitch devices, the ports that are available depend on the chassis type, for others the type of card that is configured for the card slot. Ethernet ports cannot be channelized. SONET/SDH and TDM ports can be channelized. The following types of ports are supported:

- Fast Ethernet (10/100/1000 Base-T)
- Gigabit Ethernet (1000Base-T)
- 10 Gigabit Ethernet (10000Base-T)
- 10 Gigabit Ethernet (10GBase-T)
- 40 Gigabit Ethernet (10GBase-T)
- Ethernet combo
- PoE
- OC-3/STM-1, OC-12/STM-4, OC-48/STM-16, and OC-192/STM-64 SONET/SDH
- channelized OC-3 and DS3/E3
- channelized ASAP OC-3/STM-1, OC-12/STM-4, DS1/E1, and DS3/E3

The port syntax for most devices that support daughter cards is card slot/daughtercard/port. For example, Port 1/1/1 represents port 1 of daughter card 1 in slot 1. The port syntax for the OmniSwitch is card slot/port. In every case, ports are created automatically when the daughter card is created. You must select one port object at a time and configure the properties of the port for the service that you need the port to provide. The properties vary depending on whether the port type is one of the Ethernet ports, SONET/SDH ports, TDM ports, or microwave ports. Channel objects are created on SONET/SDH or TDM ports for any type of channelization on the port whether it is a clear channel application or a sub-channel application.

Use the properties forms from the contextual menus in the navigation tree to configure port and channel parameters. You can configure the port mode as network, access, or hybrid.

- Network ports pass network-level traffic.
- Access ports are customer-facing and pass service-level traffic.
- Hybrid ports can pass network-level and access-level traffic.



Note 1 — By default, a port is in network mode.

Note 2 — See Procedure 16-2 to change the port mode.

Clear channel ports (OC-192/OC-48c/OC-12c/OC-3c) are network or access ports. Channelized ports (CHOC-12/CHOC-3c/ DS3/E3) are always in access mode, however, the ASAP CHOC-3 supports both access and network modes. The ASAP DS1/E1 ports support:

- access mode for ATM/IMA and TDM
- network mode for PPP/MLPPP

Network ports are used in the service provider transport or infrastructure network, such as an IP/MPLS-enabled backbone network or uplink ports for rings using L2 Ethernet switches. A port that is in network mode can be assigned an IP address and host an L3 interface that can perform IP routing functions.

Access ports are associated with a SAP, a subscriber, and a service to provide connectivity. Access ports and channels are configured with encapsulation values to differentiate the service on the port or channel. When a port is access mode, one or more services can be configured on the port. A channelized port that is to act as an endpoint must be in access mode. You can convert access ports to hybrid ports and migrate any existing SAPs. See Procedure 16-3 for more information.

Hybrid ports are ports that can host SAPs and network interfaces simultaneously. This enables a customer to use one uplink port for enterprise and end-user traffic. A hybrid port preserves the existing network and access port functionality, and uses the same QoS, scheduler, and port scheduler resources as other ports, but requires the configuration of weight values that allocate buffer percentages to the access and network traffic on the port.

The 5620 SAM supports hybrid mode configuration for Ethernet ports on the 7210 SAS-M (in Network mode), Release 6.0 R1or later, 7210 SAS-X, Release 6.0 R1 or later, 7450 ESS, 7750 SR-7, 7750 SR-12, and 7950 XRS.



Note — Single-slot chassis such as the 7450 ESS-1 and 7750 SR-1 do not support hybrid port mode.

You can configure a hybrid port on an Ethernet MDA in an IOM-3XP, or on a CMA in an IOM-XP. The 7750 SR supports hybrid port configuration on an IMM in addition to an IOM-3XP.



Note — Hybrid port configuration is not supported on an HSMDA or a VSM MDA.

A hybrid port supports dot1q and QinQ encapsulation, but does not support null encapsulation, in order to accommodate single-SAP operation. The available VLAN tags are shared among the VLAN SAPs and VLAN network IP interfaces. When you create a SAP or L3 interface on a hybrid port, the outer VLAN tag must not be in use by another SAP or L3 interface on the port.

By default, the MTU of a hybrid port is set to the larger of the network and access MTUs to accommodate the creation of L3 interfaces and SAPs.



Note 1 — A hybrid port can participate in a single-chassis LAG.

Note 2 — A hybrid port cannot participate in an MC-LAG or MC ring.

See the appropriate device documentation for more information about hybrid ports.

When working with a TDM port, you must specify the Line Buildout as either short or long. That is, for a DS3 port the Line Buildout parameter must be configured. If the TDM port is in the context of a SONET STS-1 sub-channel, for example, the DS3 channel is built on the STS-1 channel of a SONET port, the line buildout parameter is not required.

At the connection termination points, you are required to configure the Encap Type as required, the MTU size as required, and the configured MAC address as required when configuring the port or channel.

Policies can be added or deleted as required using the manage policy forms.

You can associate policies to ingress and egress access and network ports. Buffer policies are used to create and edit QoS buffer pool resources on network ports, access ports, and access channels. Egress network ports, access ports, and access channels have a dedicated buffer pool for queuing. The traffic is handled by a single buffer pool, one at the ingress, and one at the egress.

You can configure the amount of egress buffer space to be allocated to the port or channel. By default, all egress buffers are allocated fairly among the egress ports and channels based on their relative egress bandwidth.

The egress buffers for egress network ports and channels are put into per-port or per-channel egress buffer pools and are used by the egress network forwarding class queues on that port or channel. The ingress buffers allocated to network ports and channels are summed into a single pool and are used by the ingress network forwarding class queues (defined by the network ingress buffer policy).

The egress and ingress buffers allocated to access ports and channels are put into an egress buffer pool and ingress buffer pool for the port or channel. The access buffer pools are used by egress and ingress service queues created by the SAP-egress and SAP-ingress policies in use by services on the port or channel.

Changing the size of an egress buffer pool should be carefully planned. By default, there are no free buffers to increase the size of a pool. In order to increase a pool on one port or channel, the same amount of buffers must be freed from other egress buffer pools on the same daughter card.

Digital diagnostics monitoring

The 5620 SAM displays the following digital diagnostics monitoring data and alarm and warning information for ports on CFPs, QSFPs, SFPs and XFPs optical modular transceivers:

- temperature
- supply voltage (SFP)
- TX bias
- TX output power
- RX received optical power
- external calibration

The transceiver is programmed with warning and alarm thresholds for low and high conditions that can generate system events. The thresholds for CFPs, QSFPs, SFPs, and XFPs are programmed by the transceiver manufacturer. The 5620 SAM raises an alarm when these thresholds are exceeded.

You can view digital diagnostics monitoring information from the DDM tab and the Lane DDM tab on the property form of supported ports. The External Calibration tab is available if the ports on CFPs, QSFPs, SFPs, and XFPs optical modular transceivers support the external calibration functionality.

Tagged and untagged VLAN ports

The 5620 SAM supports tagged and untagged ports as VLAN access ports.

Table 16-1 describes the behavior when ingress tagged or untagged traffic enters and then exits a VLAN.

Table 16-1 Tagged and untagged traffic behavior

Ingress traffic configuration	Ingress VLAN port configuration	Action	Egress VLAN port configuration and action
Untagged	Untagged	The VLAN allows the traffic and passes it based on the default VLAN ID. The MAC address of the destination is learned.	If the egress VLAN port is untagged, the traffic remains untagged.
			If the egress VLAN port is tagged, a tag is added to the traffic.
	Tagged		If the egress VLAN port is untagged, the traffic remains untagged.
			If the egress VLAN port is tagged, a tag is added to the traffic.

(1 of 2)

Ingress traffic configuration	Ingress VLAN port configuration	Action	Egress VLAN port configuration and action
Tagged	Untagged	The VLAN allows the traffic if the tag matches the default VLAN ID. The MAC address of the destination is learned. If the tag does not match the default VLAN ID, the traffic is dropped.	If the egress VLAN port is untagged, the tag of the traffic is removed. If the egress VLAN port is tagged, the traffic remains tagged.
	Tagged	The VLAN allows the traffic: • if the tag matches the default VLAN ID • if the tag matches another VLAN ID The MAC address of the destination is learned. If the tag does not meet either condition, the traffic is dropped.	If the egress VLAN port is untagged, the tag of the traffic is removed. If the egress VLAN port is tagged, the traffic remains tagged.

(2 of 2)

Figures 16-1 and 16-2 show how tagged and untagged traffic is handled on the devices, based on the VLAN ID.

Figure 16-1 Untagged traffic and VLANs

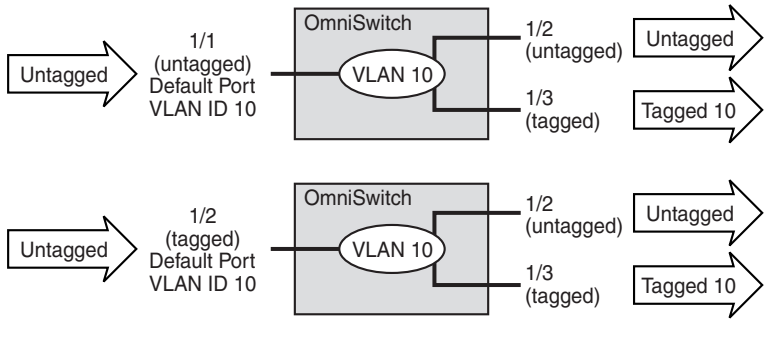
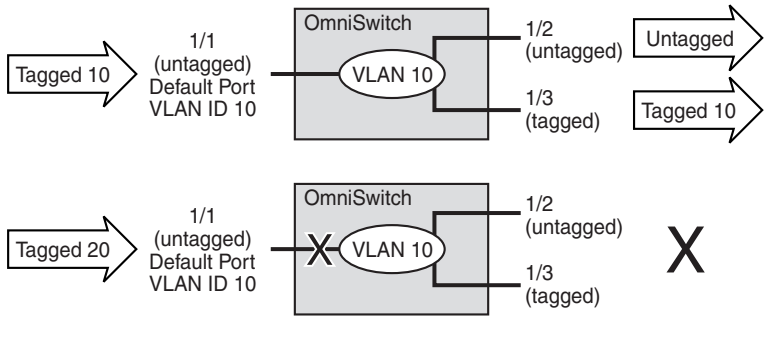


Figure 16-2 Tagged traffic and VLANs



Connection termination points for services and interfaces

Connection termination points are objects that represent terminating endpoints for a service, for example the endpoint of a VLL service. Connection termination points can be Layer 2 or Layer 3 interfaces, depending on the type of service being created. At the connection termination points you must configure the mode as Access or Network, the Encap Type as required, the MTU size as required, and the configured MAC address as required when configuring the port or channel. The following objects can be used for connection termination points:

- STS-3 to STS-192 clear channels
- DS3 clear channel
- DS0 groups
- ports
- bundle

STS-3 to STS-192 clear channel

STS-3 to STS-192 clear channel SONET/SDH ports can be used to create SAPs or IP interfaces with one clear channel on each port that operates at the rate of the parent object. Clear channel SONET applications can be performed on any OC-*n* card. SONET channel termination for 1 × 10-Gig MDAs are not supported. See "SONET clear channel applications" in this section for more information.

DS3 clear channel

A DS3 clear channel can be a connection termination point when it is explicitly configured as unchannelized, that is, when the Configuration Type is set to None, which is the default setting for a DS3. DS3 clear channel connections cannot be channelized to a lower level than the one full DS3 channel. See "TDM channelization and clear channel applications" in this section for more information.

DS0 channel groups

A TDM channel group connects a group of DS0s by allocating a specific number of spans or interfaces and channels to a group of channels. The DS0 channel group defines the incoming and outgoing parameters for a group of channels such as IP profiles, routing tables, and translation tables to be assigned during the configuration of the specific channel group.

To use a DS1 or E1, you must create at least one DS0 group for the DS1 or E1. The 5620 SAM supports the automatic configuration of sub-channels and assignment of timeslots on the ports within DS0 groups. Depending on the TDM port selected, the 5620 SAM automatically creates the DS0 channel groups with the appropriate type of timeslots. For example, you can assign timeslots to a DS0 channel group as follows:

- For DS1 channel types: Use four timeslots per channel group, which results in six DS0 channel groups with IDs from 1 to 6. Each contains four timeslots.
- For E1 channel types: Use five timeslots per channel group, which results in six DS0 channel groups with IDs from 1 to 6. Each contains five timeslots, with one timeslot not assigned.

You can view the channels that are assigned in DS0 groups using the associate properties form. You can also disable, enable, or reassign the assignment of timeslots as required, in a DS0 group.

See "TDM channelization and clear channel applications" in this section for more information about DS0 channel groups. See Procedure 16-26 for information about creating channels on ports for card types that support multiple sub-channels. See Procedure 16-31 for information about creating TDM DS1 or E1 channels and DS0 channel groups.

SONET STS-1 sub-channels

Only the DS0 group level can be used as a connection termination point for SONET STS-1 sub-channels. Channelization on the 1 × OC12 can be used to create up to 12 SONET STS-1 sub-channels. Each STS-1 channels can be used to create a DS3 frame on which you can build DS1 or E1 channels that can be configured to the DS0 channel group level. You can configure the DS0s of a DS0 group in any sequence and you do not need to use all DSOs. For example, you can use DS0 1, 3, 5, and 9. See "SONET VT1.5 and VT2 payloads" in this section for more information.

Only the DS0 group level can be used as an endpoint on the channelized 12 × DS3 card. Channelization can be used on each DS3 port of the card to create independent TDM channels in the form of DS1 or E1 data channels that handle DS0 groups. The DS0s of a DS0 group can be configured in any sequence and you do not need to use all DS0s. For example, you can use DS0 1, 3, 5, and 9. See "SONET and SDH sub-channel applications and structure" in this section for more information.

Ethernet ports

Ethernet ports can be configured as connection termination points in SAPs and IP interfaces. They cannot be channelized.

You must configure the class of port, such as fast Ethernet, GigE, or 10G Ethernet. You must also configure the port encapsulation at the connection termination point. Ethernet access ports use:

- dot1q—supports multiple services on the port; the outer encapsulation value that distinguishes services is the VLAN ID in the IEEE 802.1Q header
- QinQ—supports multiple services on the port/channel; the inner and outer encapsulation values that distinguish services is the VLAN ID in the IEEE 802.1Q header
- null—supports a single service on the port

You must configure the duplex parameter from the Ethernet tab if the port is to be added to a LAG. Configure the Dot1 Q Ethertype and Q in Q Ethertype parameters from the Ethernet tab, if required. The range is 1536 to 65 535.

You must also configure the speed parameter from the General tab. The options are 10, 100, 1000, or 10 000, depending on the speed of the Ethernet interface.

Most OmniSwitch chassis offer four hybrid or combo ports. These ports consist of four paired 10/100/1000Base-T ports and four 1000 SFP ports. Preferences for these ports are configurable and, depending on the configuration, redundancy can be provided if a link fails.

OmniSwitch learned port security

LPS provides a mechanism to control network device access on one or more OmniSwitch ports. Configurable LPS parameters allow you to restrict the source learning of host MAC addresses to:

- a specific amount of time in which the switch allows source learning to occur on all LPS ports
- a maximum number of learned MAC addresses allowed on the port
- a list of configured authorized source MAC addresses allowed on the port

The following options allow you to specify how the LPS port handles unauthorized traffic.

- Block only traffic that violates LPS port restrictions; authorized traffic is forwarded on the port.
- Disable the LPS port when unauthorized traffic is received; all traffic is stopped and a port reset is required to return the port to normal operation.

See Procedure 23-63 for information about enabling LPS on Ethernet ports and configuring LPS properties. See Procedure 16-23 for information about configuring static MAC addresses on LPS enabled Ethernet ports.



Note — A deployment error is displayed in 5620 SAM while creating a LAG with ports. This deployment failure occurs if there is an LPS/VLAN configuration done on a specific port, using CLI.

MTU size and port configuration

You must specify the MTU size for an Ethernet port using the MTU (bytes) parameter on the General tab at the connection termination endpoint.

Consider the following when you configure MTU parameters.

- The managed devices must handle MTU limitations at many service points. The physical (access and network) ports, service, and service tunnel MTU values must be individually defined.
- The ports to be designated as network ports and the ports to be designated as access ports intended to carry service traffic must be identified.
- MTU values should not be frequently modified.
- Service MTU values must be less than or equal to the service tunnel MTU.
- Service MTU values must be less than or equal to the access port MTU.
- The MTU value for an in-band management port should be less than or equal to the MTU value for the peer port connected to the in-band management port.

See the device specific documentation for end-to-end considerations for configuring maximum MTU size throughout the managed network.

The Ethernet port MTU parameter indirectly defines the largest physical packet that the port can transmit or that the far-end Ethernet port can receive. Packets received that are larger than the MTU are discarded. Packets that cannot be fragmented at egress and that exceed the MTU are discarded.

The parameters for MTU configuration include the destination MAC address, source MAC address, Ethernet encapsulation type, length field, and complete Ethernet payload.

The MTU value for a port is associated with the port mode, such as access or network, and the port encapsulation type. If you change the mode or encapsulation type value for a port, the 5620 SAM adjusts the MTU value to a default value. If you do not want the MTU values for ports to revert to the defaults, you can configure the 5620 SAM to retain the currently configured MTU values for ports regardless of a mode or encapsulation type change. See Procedure 16-4 for more information.

HSMDA Egress Secondary Shapers

The egress port scheduler combines all subscriber queues of the same scheduling class and services the queues in a byte fair round robin fashion. This results in more packets being forwarded into the aggregation network towards a DSLAM than the DSLAM can accept. If the HSMDA egress port is congested, the egress bandwidth represented by the downstream discarded packets to the DSLAM may be allocated packets destined to other DSLAMs.

The HSMDA supports egress secondary shapers to provide a control mechanism to prevent downstream overruns without affecting the class-based scheduling behavior on the port. All subscribers destined to the same DSLAM have their queue groups mapped to the same egress secondary shaper. As the scheduler services the queues within the groups according to scheduler class, the destination shaper is updated.

After the shapers rate threshold is exceeded, scheduling for all queues associated with the shaper is stopped. When the dynamic rate drops below the threshold, the queues are allowed to be placed back on the scheduler service lists. By removing the queues from their scheduling context for a downstream congested DSLAM, the port scheduler is allowed to fill the egress port with packets destined to other DSLAMs without affecting class behavior on the port.

Egress secondary shapers are configured per port.

PoE

The 5620 SAM supports Power over Ethernet on the following devices:

- 7210 SAS-T ETR; see Procedure 16-18
- 7705 SAR-H; see Procedure 16-19 and "PoE on the 7705 SAR-H"
- 7705 SAR-W; see Procedure 16-20
- OmniSwitch (except for the Metro version of the OS 6250); see Procedure 16-24

PoE provides power directly from the Ethernet ports. Powered devices such as IP phones, wireless LAN stations, Ethernet hubs, and other access points can be plugged directly into PoE-enabled Ethernet ports. The 5620 SAM supports PoE and PoE Plus on supporting devices.

PoE on the 7705 SAR-H

The 7705 SAR-H PoE functionality uses the main shelf power supply and an external power supply. The four 10/100/1000 copper ports on the main assembly have PoE capabilities. These ports are used to connect remote VoIP phones, CCTV cameras, and radios that require in-line power. Power is carried over data lines. You can configure internal or external PoE power.

Internal PoE

Two of the 10/100/1000 copper ports on the main assembly provide standard PoE (15.4 W) using the existing power supply to provide the PoE line power. Only ports 5 and 6 support PoE when the power mode is configured as internal. See Procedure 16-19 for more information.

External PoE

For an external PoE power supply, up to four PoE ports are supported. Standard PoE ports (15 W) and PoE Plus ports (34 W) can be combined to deliver up to 83 W of power. You can configure one of the following combinations:

- up to four PoE ports
- up to three PoE ports and one PoE Plus port. Only port 7 can be configured as PoE Plus.
- one PoE and up to two PoE Plus ports



Note — Ports 5 and 6, or ports 7 and 8 can only support one PoE Plus port per pair (for example, ports 5 and 6 cannot support two PoE Plus ports). Only ports 5 and 7 can be configured as PoE Plus.

See Procedure 16-19 for more information.

Moving and copying SAPs between ports

You can move and copy SAPs between physical Ethernet ports, logical ports, or a combination of both. You can also move and copy SAPs between endpoints configured with ATM encapsulation. For example, you can move a SAP on an IMA bundle to another bundle or to a TDM channel configured with ATM encapsulation. This functionality is typically used in redundancy scenarios, or to recover from a hardware failure.

Consider the following before you attempt to copy or move a SAP:

- Ports:
  - The source and destination ports can be on the same or different chassis. Inter-chassis copy or move is supported only when both NEs are of the same type, in the same chassis mode, and at the same major software release, for example, 10.0 R1 and 10.0 R3.
  - The source and destination ports can be the same. This configuration allows you to change the encapsulation values for a group of SAPs on the same port using outer and inner encapsulation offset values. These values can be positive or negative, depending on whether the encapsulation values must increase or decrease.
  - The physical Ethernet ports can be of different types; for example, Fast Ethernet (10/100/1000 Base-T), Gigabit Ethernet (1000 Base-T), and 10 Gigabit Ethernet (10 GBase-T).
  - The source and destination ports must be configured as access ports.
  - The encapsulation type must be the same on the source and destination ports.
  - You cannot copy or move a SAP between an HSMDA port and a non-HSMDA port.
- SAPs:
  - The SAPs can be associated with either L2 access interfaces on services such as Apipes, Epipes, Ipipes, VPLS, and MVPLS, or L3 access interfaces or subscriber interfaces that are associated with services such as IES and VPRN.
  - The copy and move operation does not copy and move MEPs that are configured on a VPLS, MVPLS and Epipe L2 access interface. MEP configuration is discarded during the copy and move operation.
  - For L2 and L3 access interfaces, you can move all SAPs or a subset of the SAPs on a port. You can also copy all SAPs or a subset of the SAPs on a port for L2 access interfaces.
  - All SAPs associated with a specific port within a group interface contained in an L3 subscriber interface can be moved at the same time.
  - The copy and move operations fail if the encapsulation value for a SAP on the source port is used by a SAP on the destination port. You can modify the SAP encapsulation values used on the destination port, if required.
  - The selected SAPs on the source port do not need to belong to the same service.
  - If a SAP on the source port belongs to a service not supported on the destination port, the SAP is not copied or moved.
  - The maximum number of SAPs varies for ports and MDAs. The SAP copy or move operation fails if the SAP capacity is exceeded for the destination port.
  - You cannot change SAP encapsulation from bridged to routed if ARP and DHCP options have been configured.
- SAP attributes:
  - VPLS and MVPLS dynamic FIB entries that are associated with copied or moved SAPs are discarded. Static FIB entries are transferred to the destination port after a successful SAP copy or move.
  - All SAP redundancy relationships at the source port, such as those provided by an MVPLS, are discarded during a copy or move operation.
  - All alarms, statistics, or OAM test results that are associated with a copied or moved SAP are discarded.

- When a source SAP belongs to an SHG, the 5620 SAM attempts to preserve the SHG membership. The destination SHG must have the same name as the source SHG, and must have the same residential SHG status. If an SHG with the same name does not exist on the destination service site, the 5620 SAM creates it.
- When a source SAP is uses an aggregation scheduler, the scheduler is copied to the destination. The aggregation scheduler must be unique to the destination NE and must have the same scope, for example, MDA or port.

See Procedures 16-5, 16-6, and 16-7 to move access interface SAPs between ports.

SONET/SDH and TDM port encapsulation

SONET/SDH and TDM ports can be configured as connection termination points in SAPs and IP interfaces. They can be channelized.

An access port is used for customer-facing traffic on which services are configured. SAPs can only use an access port. When a port is configured for access mode, the appropriate encapsulation type must be specified to distinguish the services on the port.

You must configure the Encap Type parameter from the General tab at the connection termination point. SONET/SDH or TDM ports or channels support the following encapsulation types, depending on the MDA type:

- BCP Null
- IPCP
- BCP Dot1 Q
- FR — Support multiple services using the DLCI header to distinguish services
- ATM — Support multiple services using the VCI or VPI of the PVC
- PPP Auto
- CEM

MTU size considerations apply to SONET/SDH and TDM channels. See "MTU size and port configuration" in section 16.2 for more information.

SONET clear channel applications

Ports on OC-*n* cards can be used for SONET clear channel applications. SONET or TDM clear channel applications allow you to create a full channel on a port which can be configured as access or network mode for SONET and access only for TDM. For example, when you create a 16 × OC3 SFP card, 16 ports are created. You can create one full channel on each of these ports. For more information about the 4-port OC3/STM1 ASAP SFP card for clear channel support on the 7705 SAR-8, see OC3/STM1 clear channel support on the 7705 SAR-8 and 7705 SAR-18 in this section.

STS-192/48/12/3 clear channel applications use the following syntax:

```
card slot/daughtercard/port.STSType
```

For example, the clear channel STS-12 on slot 4, MDA 1, port 1 is named 4/1/1.sts12

Table 16-2 lists available SONET channel applications and parameters for clear channel, sub-channel, and TDM applications.

Table 16-2 SONET channel parameters

Applications	Channel ranges								
	STS-192	STS-48	STS-3	STS-1	DS3	DS1	DS0	E1	DS0
SONET Clear channel	1	1	1		1				
SONET Sub channel			1 to 4	1 to 3	1	1 to 28	1 to 24	1 to 21	2 to 32
TDM					1	1 to 28	1 to 24	1 to 21	2 to 32

OC3/STM1 clear channel support on the 7705 SAR-8 and 7705 SAR-18

The 7705 SAR-8 and 7705 SAR-18 support the 4-port OC3/STM1 ASAP SFP card. The 4-port OC3/STM1 ASAP SFP card has four SFP-based ports that can be independently configured for ATM in access mode or for Packet over SONET/SDH (POS) in network mode. Each port can be independently configured to be SONET (OC3) or SDH (STM1) framing. See ATM encapsulation in this section for more information. The interface must be configured as UNI. The transmit clock rate for a port can be device- or loop-timed.

The section trace (J0) byte can be configured by the operator to check the physical cabling. The port can activate and deactivate local line and internal loopbacks. The MTU size for a 4-port OC3/STM1 ASAP SFP access port is fixed at 1572 for ATM encapsulation.

CSM activity switches for a 4-port OC3/STM1 ASAP SFP card on the 7705 SAR-8 and 7705 SAR-18 are hitless on the data path.

The 7705 SAR-8 and 7705 SAR-18 support the 2-port OC3/STM1 ASAP SFP card. The 2-port OC3/STM1 ASAP SFTP card has two SFP-based ports (optical or electrical) that can be configured for ATM/IMA or TDM in access mode or for MLPPP in access or network mode. The port type must be configured to be either SONET (OC3) or SDH (STM1).



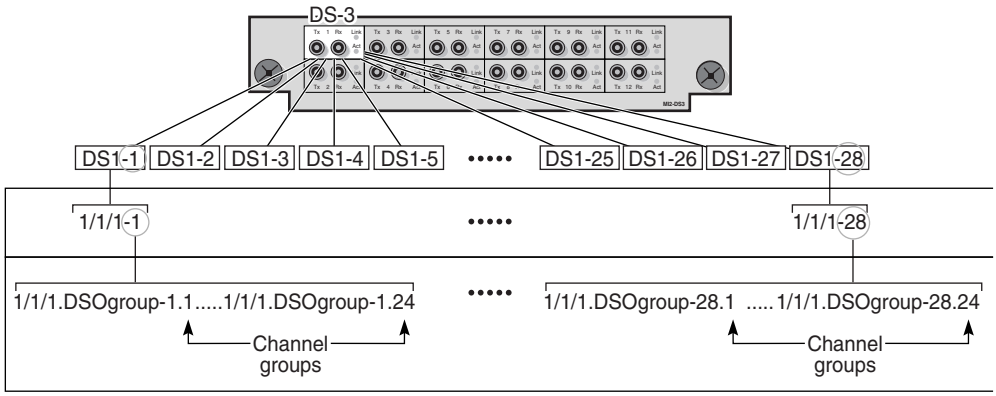
Note — Channels on the 4-port OC3/STM1 ASAP SFP adapter card cannot be configured as IES SAPs.

TDM channelization and clear channel applications

When you create a 4 or 12 ×DS3/E3 card, 4 or 12 DS3/E3 ports are created. You can then create DS3/E3 channels using the 5620 SAM, one per port. Each DS3/E3 channel can be channelized into 28 independent DS1 or 21 independent E1 data channels or, in clear channel applications, the DS3 can be the connection termination point. For channelized DS3 connections, each DS1 channel can be channelized to 24 DS0 groups and each E1 channel can be channelized to 31 DS0 groups. To use a DS1 or E1, you must create at least one DS0 group for the DS1 or E1.

By default, DS3 ports are automatically created for clear channel connections. To create a channelized DS3, you must configure the DS3 channel type as E3 or DS3 on the port. To channelize the DS3 to the DS0 level, you must set the Channelization Type to Channelized DS1 or E1. Figure 16-3 shows the channelized DS3 port structure for DS1 channels.

Figure 16-3 Channelized 12 × DS3 port structure for DS1 Channels



The channelized DS3 port structure for E1 channels has the following parameter values:

- each DS3 port supports 21 E1 channels
- each E1 channel supports 31 DS0 channel groups

TDM-based DS3 channelization uses the following syntax:

DS3 channel configured for TDM:

```
card slot/daughtercard/port.DS3-
```

DS1 channel from a TDM-based DS3 channel:

```
slot/daughtercard/port.DS1-[DS3#].[DS1#]
```

E1 channel from a TDM-based DS3 channel:

```
slot/daughtercard/port.DS1-[DS3#].[E1#]
```

DS0 group channel from the DS1 channel:

```
slot/daughtercard/port.DS0Grp-[STS3#].[STS1#].[DS1#/E1#].[Group#]
```

Table 16-3 provides an example of the naming conventions for a 12 × DS3 port.

Table 16-3 Example of TDM channel naming convention

Syntax	Description	Additional information
Channel 1/1/1.ds3	1/1/1 is the slot number/daughtercard number/port number .ds3 identifies the channel as DS3	Because DS3s are unchannelized by default, you must configure the Channelization Type as Channelized.
Channel 1/1/1.ds1-1.2	.ds1 identifies the channel as DS1 1 is the DS3 number .2 is the DS1 number (1 to 28)	Identifies the DS1 channel and shows how the DS3 level acts as a place holder for the DS1s.
Channel 1/1/1.e1-1.2	.e1 identifies the channel as E1 1 is the DS3 number .2 is the E1 number (1 to 21)	Identifies the E1 channel and shows how the DS3 level acts as a place holder for the E1s.
Channel 1/1/1.ds0Grp-1.2.23	.ds0Grp- identifies the channel as a DS0 group 1 is the DS3 number .2 is the DS1 number (1 to 28) or E1 number (1 to 21) .23 identifies the DS0 channel group (1 to 24) on the DS1 or (2 to 32) on the E1	The DS0 group is configured on the DS1 or E1 channel. Only a DS0 can be used as a CTP.

ATM encapsulation

SONET/SDH clear channels can be provisioned so that ATM cells are encapsulated in SONET/SDH frames. The entire SONET/SDH path of the port is then used to carry ATM cells. The channel of the port becomes the ATM interface. ATM encapsulation is supported on the following daughter cards:

- 16 × ATM OC3 SFP
- 16 × ATM OC3 SFP B
- 4 × ATM OC12/OC3 SFP
- 4 × ATM OC12/OC3 SFP B
- 4 × OC3/STM1 ASAP SFP
- 4 × Any Service Channelized OC3
- 16 × Any Service Channelized DS1/E1

SONET/SDH clear channel applications with ATM encapsulation use the following syntax:

```
Daughter Card Slot - 3 (16 × ATMOC3), OK

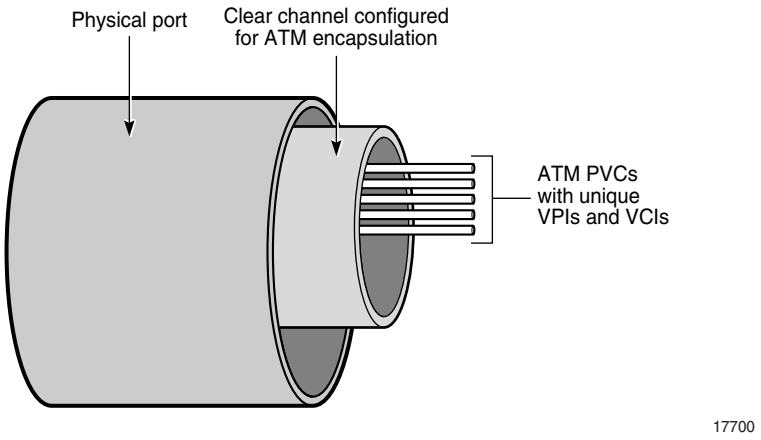
Port 3/1/1 - Speed: OC3, State: OK

Channel 3/1/1.sts3, Mode: Access, Encap: ATM, State: Ok
```

Customer devices with ATM interfaces are connected directly or using the ATM access network to a 7750 SR that offers IES or VPRN services.

A SONET/SDH clear channel with ATM encapsulation can carry multiple ATM PVCs. ATM PVCs cannot be created from the 5620 SAM. They are created automatically by the router when a new Layer 3 interface over ATM is created. Figure 16-4 shows an example of ATM PVCs on a SONET/SDH clear channel.

Figure 16-4 ATM PVCs on a SONET/SDH clear channel



ILMI links between ATM interfaces

ILMI links can be configured between ATM interfaces. ILMI is a protocol that sets and sends physical layer, ATM layer, virtual path, and virtual channel parameters that are exchanged by ATM interfaces.

When ILMI is run between two ATM interfaces, the interfaces exchange ILMI packets that consist of SNMP messages across the physical connection. An ILMI link allows ILMI to run on an available virtual channel. When an ILMI link is created to carry ILMI messages, a PVC is automatically created with default PVC attributes. The PVC is deleted when the ILMI link is removed.

IMA

IMA is supported on channelized ASAP MDAs on the 7750 SR, 7710 SR, 7705 SAR, and ATM DS1/E1 CMA on the 7710 SR. For 9500 MPR/9500 MPRe device IMA support, see the *5620 SAM MPR User Guide*.

IMA group bundles aggregate E1 or DS1 ATM paths into a single logical ATM interface. Each IMA group bundle can have from 1 to 8 members, or links. Up to 56 IMA group bundles can be configured on a single 7750 SR or 7710 SR MDA. Up to 8 IMA group bundles can be configured on a single 7705 SAR daughter card.

Each ATM Interface supports up to 48 VP/VC connection points. Each 16 × E1 ASAP Access (ETSI) board supports up to 128 VP/VC connection points.

An IMA group bundle has the following common interface properties:

- ATM encapsulation type is displayed on the ATM Interface properties form by clicking on the “Edit ATM button”.
- MTU value (of the primary link)

Member links inherit the common properties of the IMA group to which they belong. Only the properties of the primary link can be changed. The primary link is the member with the lowest interface index or initialization sequence. The primary link may change as member links are added and deleted from the IMA group.

Consider the following when you create a multilink IMA group bundle.

- When a path becomes a member of an IMA group bundle, it is no longer a physical ATM path interface.
- The members of the IMA group bundle inherit all of the properties of the primary link, such as the SONET configuration and MTU. If you modify the configuration of the primary link, the configuration of the bundle members is also modified.
- Member links that are added after the primary link has been added to the IMA group bundle must match the configuration of the primary link.
- You cannot configure services on a member link.

16.3 SONET and SDH sub-channel applications and structure

SONET sub-channel applications allow you to create multiple STS-1 channels on deep channelized OC-12 and OC-3 ports, and to configure multiple DS0 connection termination points.

An STS-1 sub-channel is configured, or channelized, to carry one of the following payload types:

- DS3
- VT1.5
- VT2

Because of the differences between SONET and SDH in multiplexing and mapping of tributary payloads into higher digital levels, some building blocks of SDH have no SONET equivalent and therefore the containment hierarchy and terminology for SDH is different from SONET. See "Comparison of SONET and SDH hierarchies" and "SDH AU-4 and AU-3 sub-channel applications" in this section.

SONET DS3 payload

The following example, illustrated in Figure 16-5, shows the channelization sequence for a DS3 payload on a 1 × OC12 Deep Channel card.

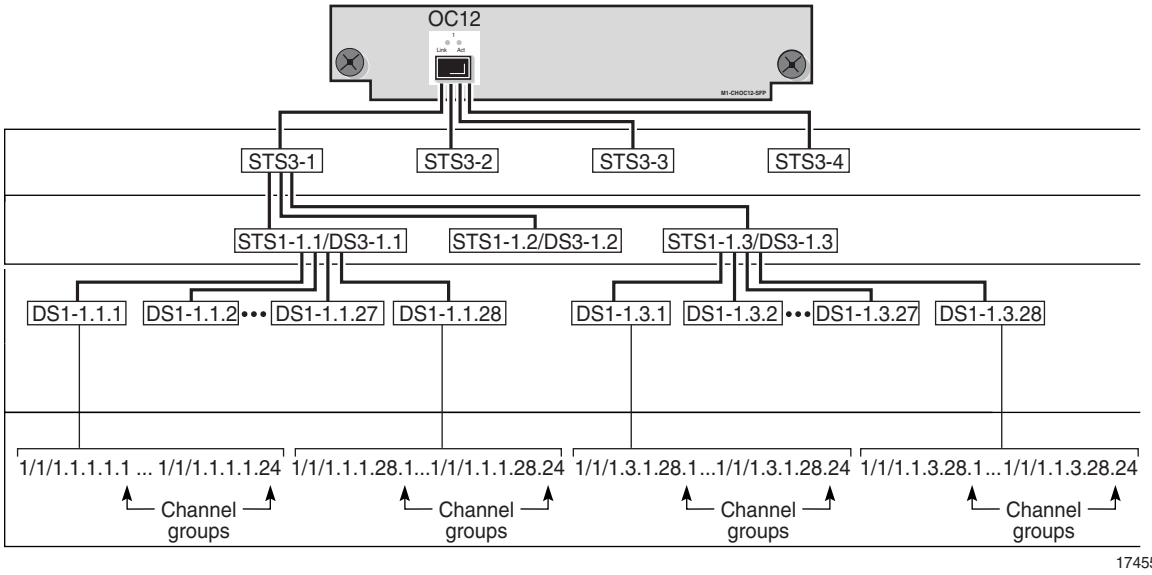
1 One OC-12 port is created when you create a channelized 1 × OC12 Deep Channel card.

2 This port can be channelized into 12 SONET STS-1 sub-channels from the four STS-3s available on the port.

3 You can then configure each of these STS-1s to carry a DS3 frame

4 Each DS3 frame can be channelized into 28 independent DS1 data channels or 21 independent E1 data channels. Each channel must be created one at a time.

Figure 16-5 Channelized 1 × OC-12 port structure using STS-1/DS3 sub-channels



SONET VT1.5 and VT2 payloads

The following example, illustrated in Figure 16-6, shows the channelization sequence for a VT1.5 or VT2 payload on a 1 × OC12 Deep Channel card.

1 One OC-12 port is created when you create a channelized 1 × OC12 Deep Channel card.

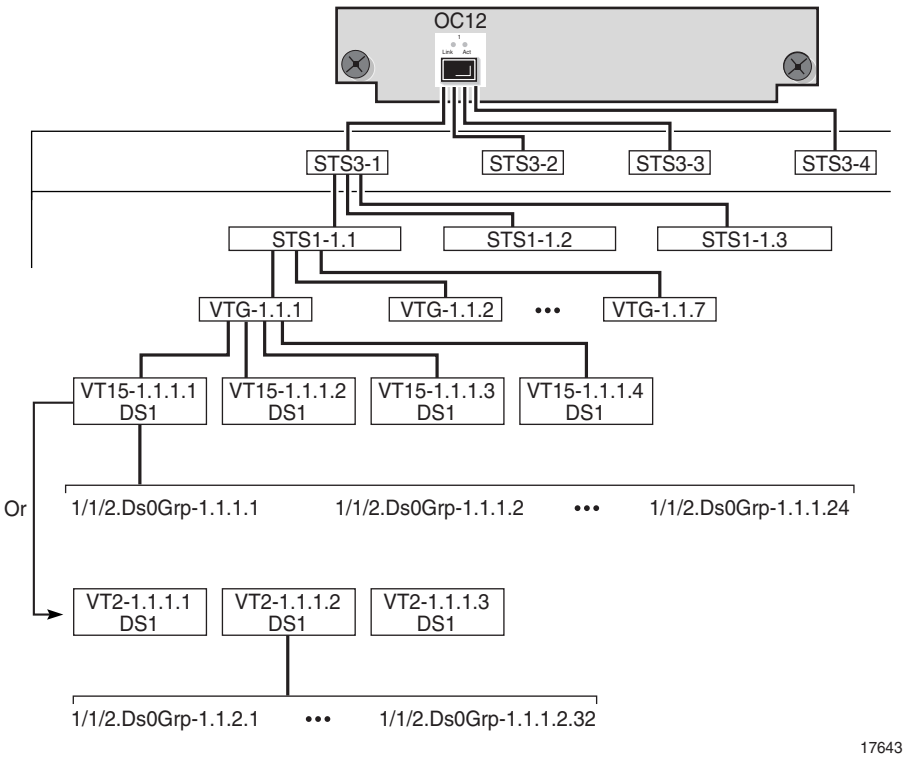
2 This port can be channelized into 12 SONET STS-1 sub-channels from the four STS-3s available on the port.

3 You can then configure each of these STS-1s to be channelized to carry up to 28 DS1. For SONET sub-channel configuration you must select payload type VT1.5 or VT2. When you choose VT1.5 payload type, seven VTG are implicitly created.

4 Each VTG is channelized into four independent VT1.5 channels or three VT2 channels, each of which can carry an independent DS1 data channel. Each channel must be created one at a time.

5 Each VT1.5 DS1 channel can be configured to handle up to 24 DS0 groups. Each VT2 DS1 channel can be configured to handle up to 32 DS0 groups. To use a DS1, you must create at least one DS0 group for the DS1 or E1.

Figure 16-6 Channelized 4 × OC-3 port structure using VT sub-channels



SONET sub-channel syntax

The 5620 SAM uses the following SONET syntax for the STS-1 sub-channel:

```
card slot/daughtercard/port.STS1-[STS3#].[STS1#]
```

DS3 channels from an STS-1 sub-channel use the following syntax:

```
slot/daughtercard/port.DS3-[STS3#].[STS1#]
```

DS1 channels from a DS3 channel use the following syntax:

```
slot/daughtercard/port.DS1-[STS3#].[STS1#].[DS1#]
```

E1 channels from a DS3 channel use the following syntax:

```
slot/daughtercard/port.DS1-[STS3#].[STS1#].[E1#]
```

VT15 or VT2 from a VT group use the following syntax:

```
slot/daughtercard/port.VTG#-[STS3#].[STS1#]
```

DS1 channels from a VT15 or VT2 use the following syntax:

```
slot/daughtercard/port.DS1-[STS3#].[STS1#].[VT15#] or
[VT2#}.[VTG#].[DS1#]
```

Table 16-4 shows an example of the SONET sub-channel syntax.

Table 16-4 Example of SONET sub-channel syntax for an OC-12 port

Syntax	Description	Additional information
Channel 1/1/1.sts1-2.2	1/1/1 is the slot number/daughtercard number/port number 2 is the STS-3 number (1 to 4) .2 is the STS-1 number (1 to 3)	The sts1 parameter is 2.2 which means that it is the fifth STS-1. There are four STS-3s for an OC-12 and each STS-3 has three STS-1s such that the fifth STS-1 is the second STS-1 of the second STS-3.
Channel 1/1/1.ds3-2.2	.ds3-2 is the STS3 number (1 to 4) .2 identifies the STS-1 number (1 to 3)	Identifies the DS3 channel and shows how the sts1 level acts as a place holder for the DS3
Channel 1/1/1.ds1 2.2.25	.ds1-2.2.25 identifies a DS1 channel (1 to 28) on the DS3	The DS1 is configured on the DS3.
Channel 1/1/1.e1 2.2.21	.e1-2.2.21 identifies a E1 channel (1 to 21) on the DS3	The E1 is configured on the DS3.
Channel 1/1/1.DS0Grp-2.2.20.5	.DS0Grp-2.2.20.5 identifies one of the DS0 channel groups: 1 to 28 for DS1; 2 to 32 for E1	The DS0 is configured on the DS1 or E1 channel.
Channel 1/1/1.ds1 2.2.3.18	ds1 2.2.3.18 identifies a DS1 channel on the VT15 or VT2 payload, where 3 is the VT group.	—

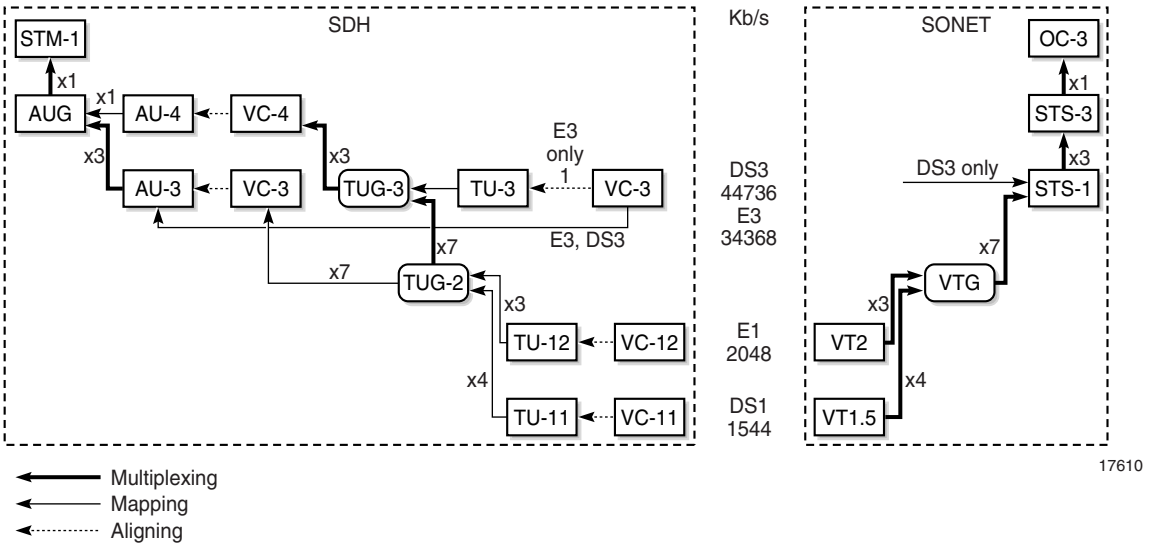
Comparison of SONET and SDH hierarchies

SONET and SDH are compatible digital hierarchies that support identical transmission rates with similar framing structures. However, SONET and SDH standards differ in the way they multiplex and map tributary payloads into higher digital levels. Because of these differences, some SDH framing blocks do not have equivalent blocks in SONET.

SONET provides one STS sub-channel, the STS-1, for mapping lower-capacity, deep-channel payloads while SDH provides two alternative sub-channels, the AU3 and the AU4. After an AU3 sub-channel is created, an AU4 cannot be created on that port in the case where the port is an OC-3 (STM-1). Conversely, if an AU4 sub-channel is created, an AU3 cannot be created on that port in the case where the port is an OC-3 (STM-1).

SONET and SDH transmission rates converge at 155.520 Mb/s where the SONET STS-3c is equivalent to the SDH STM-1 bit rate. For lower-capacity payloads, such as DS1, E1, DS3, and E3, SONET provides one unique mapping path for each payload while SDH permits two alternative paths for each payload as shown Figure 16-7.

Figure 16-7 Supported SONET/SDH multiplexing structures



SDH AU-4 and AU-3 sub-channel applications

SDH sub-channel applications allow you to create AU4 or AU3 channels on deep channelized OC-12 (STM-4) and OC-3 (STM-1) ports, and to configure multiple DS0 connection termination points.

After an AU4 sub-channel is created, it implicitly contains three TUG-3 groups. A TUG-3 is channelized to carry one of the following payload types:

- TU3
- TU11
- TU12

After an AU-3 sub-channel is created, it is channelized to carry one of the following payload types:

- DS3, E3
- TU11
- TU12

SDH TU3 payload

The following example, illustrated in Figure 16-8, shows the channelization sequence for a TU3 payload on a 4 × OC3 Deep Channel card.

1 Four OC-3 ports are created when you create a channelized 4 × OC3 Deep Channel card.

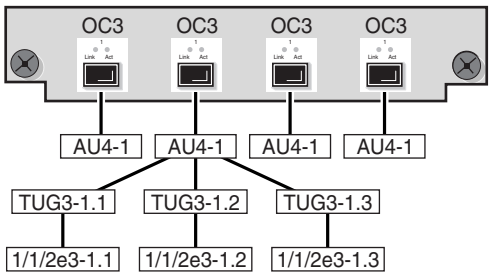
2 The user creates each required AU4 sub-channel.

3 Each AU4 sub-channel implicitly contains three TUG3 groups.

4 You can then configure each TUG3 to carry a TU3 frame

5 Each TU3 frame is channelized into an independent E3 data channel and cannot be changed.

Figure 16-8 Channelized 4 × OC-3 port structure using AU4/TU3 sub-channels



SDH E3 or DS3 payload

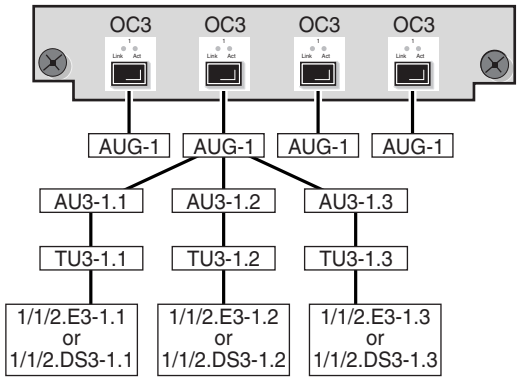
The following example, illustrated in Figure 16-9, shows the channelization sequence for an E3 or DS3 payload on a 4 × OC3 Deep Channel card using AU3 sub-channels.

1 Four OC-3 ports are created when you create a channelized 4 × OC3 Deep Channel card.

2 Each port can be channelized into up to three AU3 sub-channel.

3 Each AU3 frame can be channelized into an independent E3 or DS3 data channel.

Figure 16-9 Channelized 4 × OC-3 port structure using AU3/E3 sub-channels



SDH TU11 and TU12 payloads

TU11 and TU12 payloads can be channelized using an AU4 sub-channel or an AU-3 sub-channel. An AU4 sub-channel implicitly contains three TUG3 groups. A TUG3 and an AU3 channelized to carry TU11 or TU12 payloads implicitly contain seven TUG2 tributary groups.

The following example, illustrated in Figure 16-10, shows the channelization sequence for a TU11or a TU12 payload on a 4 × OC3 Deep Channel card.

1 Four OC-3 ports are created when you create a channelized 4 × OC3 Deep Channel card.

2 Each port can be channelized into one AU4 sub-channel or three AU3 sub-channels.

3 Each AU4 sub-channel implicitly contains three TUG3 groups.

4 You can then configure each TUG3 group or each AU3 sub-channel to carry a TU11 or TU12 payload.

5 Each TUG3 group or AU3 sub-channel implicitly contains seven TUG2 tributary groups.

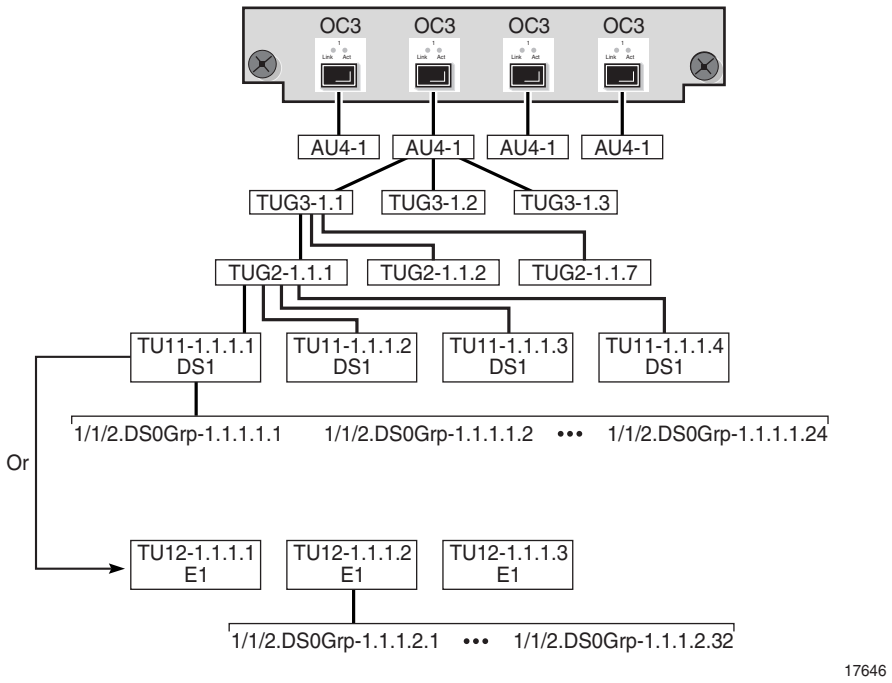
6 Each TUG2 group can be channelized into three independent TU12 channels or four independent TU11 channels.

7 Each TU12 can contain an E1 or DS1 data signal. Each TU11 can contain a DS1 data signal. Each E1 can be configured to handle up to 31 DS0 groups. Each DS1 can be configured to handle up to 24 DS0 groups. To use an E1 or a DS1, you must create at least one DS0 group for the DS1 or E1.



Note — On the same TUG3 or AU3, you cannot mix TU-1*X* with DS1 and E1 payload types. Every TU-1*X* on the same TUG3 or AU3 must use the same payload type, either E1 or DS1, not a mix of both. The mix is shown in for illustrating the structure.

Figure 16-10 Channelized 4 × OC-3 port structure using AU4/TU sub-channels



16.4 Workflow to manage port objects

The following workflow describes the sequence of high-level tasks required to manage and configure port objects. This workflow assumes that the physical devices have been installed, commissioned, and discovered. See chapter 9 for more information about device commissioning. See chapter 10 for more information about device discovery.

Note — After they are configured, port objects can be accessed using the equipment navigation tree. See chapter 5 for more information about using the equipment navigation tree. for more information.

1 As required, configure Ethernet ports; see Procedure 16-1.

2 As required, change the port mode; see Procedure 16-2.

3 As required, migrate SAPs from access mode to hybrid mode; see Procedure 16-3.

4 As required, configure the 5620 SAM to retain non-default port MTU values; see Procedure 16-4.

5 As required, copy or move L2 access interface SAPs between ports; see Procedure 16-5.

6 As required, move L3 access interface SAPs within or between ports on the same NE; see Procedure 16-6.

7 As required, move L3 subscriber interface SAPs between ports on the same NE; see Procedure 16-7.

8 As required, add a queue group to an Ethernet port; see Procedure 16-8.

9 As required, configure SONET ports; see Procedure 16-9.

10 As required, configure an HSMDA port scheduler override; see Procedure 16-10.

11 As required, configure TDM DS3 ports; see Procedure 16-11.

12 As required, configure serial ports; see Procedure 16-12.

13 As required, configure PW ports; see Procedure 16-13.

14 As required, configure ports on 7210 SAS devices, as follows:

- **a** Configure a 7210 SAS-M channelized TDM DS1 or E1 port; see Procedure 16-14.
- **b** Assign policies to a 7210 SAS Ethernet port; see Procedure 16-15.
- **c** Configure an SHG for 7210 SAS NEs; see Procedure 16-16.

15 As required, configure ports on 7705 SAR devices, as follows:

- **a** virtual Ethernet ports on a 7705 SAR 2-port ring MDA; see Procedure 16-17.
- **b** PoE ports on a 7705 SAR-H daughter card; see Procedure 16-19.
- **c** PoE ports on a 7705 SAR-W daughter card; see Procedure 16-20.
- **d** 7705 SAR ASAP channelized TDM port; see Procedure 16-21.

16 As required, configure a 7710 SR channelized TDM DS1 or E1 port; see Procedure 16-22.

17 As required, configure the following on OmniSwitch devices:

- **a** OmniSwitch Ethernet ports; see Procedure 16-23.
- **b** OmniSwitch PoE ports; see Procedure 16-24.

16.5 Workflow to manage channel objects

The following workflow describes the sequence of high-level tasks required to manage and configure channel objects. This workflow assumes that the physical devices have been installed, commissioned, and discovered, and that the port objects have been configured. See chapter 9 for more information about device commissioning. See chapter 10 for more information about device discovery.



Note — After they are configured, channel objects can be accessed using the equipment navigation tree. See chapter 5 for more information about using the equipment navigation tree.

1 As required, configure SONET clear channels; see Procedure 16-25.

2 As required, create channels on ports for card types that support multiple sub-channels; see Procedure 16-26.

3 As required, configure SONET sub-channels; see Procedure 16-27.

4 As required, configure SDH sub-channels; see Procedure 16-28.

5 As required, create VT15 (TU11) or VT2 (TU12) sub-channels; see Procedure 16-29.

6 As required, create TDM DS1 channels; see Procedure 16-32.

7 As required, configure TDM DS1 or E1 channels; see Procedure 16-31.

8 As required, configure serial channels; see Procedure 16-32.

9 As required, create TDM DS3 channels; see Procedure 16-33.

10 As required, configure TDM DS3 channels; see Procedure 16-34.

11 As required, configure a DS3 or E3 channel as a network interface on a channelized ASAP MDA; see Procedure 16-35.

12 As required, configure an L3 interface on a DS3 or E3 channel on a channelized ASAP MDA; see Procedure 16-36.

13 As required, configure a PVC; see Procedure 16-37.

14 As required, create an ILMI link; see Procedure 16-38.

15 As required, modify an ILMI link; see Procedure 16-39.

16.6 Port configuration procedures

Use the following procedures to manage ports using the navigation tree.

Procedure 16-1 To configure Ethernet ports

Perform this procedure, as required, depending on the daughter card and port type that you are configuring. Different card types display different port configuration parameters.



Note — Before you can configure 802.1X on an Ethernet access port, 802.1X must be enabled on the device and an 802.1X policy must be created and distributed to the device.

See Procedure 13-8 for information about enabling 802.1X on a device. See chapter 50 for information about creating and distributing 802.1X policies.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the port object where you want to configure an Ethernet port. The path is Network→*NE*→Shelf→Card Slot *n*→Daughter Card Slot *n*→Port *n*/*n*/*n*.

3 Right-click on the Port icon and choose Properties. The Physical Port (Edit) form opens with the General tab displayed.

4 Configure the parameters:



Note — Only the parameters that are supported on the NE, daughter card, or port are displayed.

- Description
- Configured MAC
- Mode
- L2Uplink
- Encapsulation Type
- Speed
- MTU (bytes)
- DDM Event Suppression
- Load Balance Algorithm
- Hold Time Up (seconds)
- Hold Time Down (seconds)
- Ingress Percentage of Rate (%)
- Egress Percentage of Rate (%)
- Default VLAN
- Channel
- Rx Decision Threshold Voltage Adjustment
- Optical Transport Channel Unit
- Current OLC State
- Revert OLC State

Only one MAC address can be assigned to a port. When a new MAC address is configured while the port is operational, IP issues an ARP, if appropriate, and BPDUs are sent with the new MAC address. A default MAC address is assigned by the system.

If the port is a LAG member, the Hold Time Up (seconds) parameter is configurable only if the port is the primary member. The Hold Time Down (seconds) parameter is not configurable when the port is a LAG member.

The DDM Event Suppression parameter is configurable only on ports on SFPs and XFPs optical modular transceivers.

When you set the Mode parameter to Hybrid, you cannot set the Encapsulation Type parameter to Null.

The MTU value for a port is associated with the port mode and the port encapsulation type. By default, the MTU of a hybrid port is set to the larger of the network and access MTUs.

5 If you set the Mode parameter to Hybrid, configure the following parameters in the Hybrid Ingress Buffer Allocation panel. Otherwise, go to step 8:

- Access Weight
- Network Weight

6 If you set the Mode parameter to Hybrid, configure the following parameters in the Hybrid Egress Buffer Allocation panel:

- Access Weight
- Network Weight

7 If you change the Mode parameter from Access to Hybrid and there are SAPs on the port, perform Procedure 16-3 to migrate the SAPs.

8 If you are configuring a 7210 SAS Ethernet port you can add the port to an SHG. See Procedure 16-16 for information about creating a 7210 SAS SHG.

i Click on the Select button in the Split Horizon Group panel. The Select Split Horizon Group - Physical Port list form opens.

ii Choose an SHG and click on the OK button. The Select Split Horizon Group - Physical Port list form closes, and the Physical Port (Edit) form refreshes with the SHG name.



Note 1 — A port cannot be added to or deleted from an SHG if it has a SAP configured on it or is a member of a LAG.

Note 2 — A port cannot belong to more than one SHG; you must remove any SHGs from the port before you can add the port to a different SHG.

9 Configure the Named Pool Buffer Policy for the port.

i Click on the Select button beside the Name parameter in the Ingress Pool Policy panel. A Select Ingress Pool Policy form opens with a list of ingress pool policies.

ii Choose a policy from the list.

iii Click on the OK button, the Select Ingress Pool Policy form closes and the Name parameter refreshes with the selected policy.

iv Click on the Select button beside the Name parameter in the Egress Pool Policy panel. A Select Egress Pool Policy form opens with a list of egress pool policies.

v Choose a policy from the list.

vi Click on the OK button, the Select Egress Pool Policy form closes and the Name parameter refreshes with the selected policy.

vii Configure the parameters:

- Egress Percentage of Rate (%)
- Ingress Percentage of Rate (%)



Note — Ensure that the named pool mode is enabled. See Procedure 15-28 in chapter 15 for more information.

10 Click on the States tab.

11 Configure the Administrative State parameter.

12 Click on the Policies tab. The Policies form opens with the General tab displayed.



Note — The types of policies that you can choose depend on the type of NE, daughter card, and the mode type of the port you are configuring.

- The Network Queue and Accounting Policies panel are only displayed for network and hybrid ports.
- The Port Scheduler panel is only displayed for ports on non-HSMDA daughter cards.
- The HSMDA Egress Scheduler panel is only displayed for ports on HSMDA daughter cards.

13 Click on the Select button in the Accounting Policy panel to assign an accounting policy to the port, if applicable. The Select Accounting Policy - Physical Port form opens.

14 Choose an accounting policy from the list and click on the OK button. The Select Accounting Policy - Physical Port form closes.

15 Configure the Collect Accounting Statistics parameter, if required.

16 If you are configuring an access port on a 7210 SAS-E for the collection of packet forwarding statistics on egress queues, configure the parameters in the Egress Packets Forwarding panel:

- Queue 1
- Queue 2
- Queue 3
- Queue 4
- Queue 5
- Queue 6
- Queue 7
- Queue 8

For the 7210 SAS-E, access ports always contain eight queues. You can enable up to eight queues on any port for the collection of packet forwarding statistics. However, only eight counters can be enabled for each 7210 SAS-E device. If no queues are enabled on a port, no accounting statistics are collected for that port.

17 If you are configuring a 7210 SAS Ethernet port, perform Procedure 16-15, then go to step 24.

18 Click on the Select button in the Network Queue panel to assign a network queue policy to the port, if applicable. The Select Network Queue Policy - Physical Port form opens.

19 Choose a network queue policy from the list and click on the OK button. The Select Network Queue Policy - Physical Port form closes.

20 Click on the Select button in the Port Scheduler Policy panel to assign a port scheduler policy to the port, if applicable. The Select Port Scheduler Policy - Physical Port form opens.

21 Choose a port scheduler policy from the list and click on the OK button. The Select Port Scheduler Policy - Physical Port form closes.

22 Click on the Select button in the HSMDA Egress Scheduler Policy panel to assign a scheduler policy to the port, if applicable. The Select HSMDA Egress Scheduler Policy - Physical Port form opens.

23 Choose a policy from the list and click on the OK button. The Select HSMDA Egress Scheduler Policy - Physical Port form closes.

24 Click on the DDM tab to view digital diagnostics monitoring information, if required.

25 Click on the Media Adaptor tab to view information about the SFP, if required.

26 Click on the Ethernet tab. The Ethernet port configuration form opens with the General tab displayed.

27 Configure the parameters:



Note — Only the parameters that are supported on the NE, daughter card, or port are displayed.

- Duplex
- Auto-negotiate
- Dot1 Q Ethertype
- QinQ Ethertype
- Down When Looped
- Keep Alive Interval (Sec)
- Retry Timeout (Sec)
- Use Broadcast Address
- Ingress Rate (Mbps)
- Egress Scheduler Mode
- CFM LoopBack Mode
- CFM LoopBack VLAN Range
- Connector Type
- Timestamp Capable
- Egress Rate (Kbps)
- Egress Unshaped SAP CIR (kbps)
- Egress Max-Burst
- Ingress CBS
- LACP Tunnel
- Src Pause
- Flow
- Down On Internal MAC Tx Error
- IP MTU (bytes)
- Port Clock Mode
- XGig Mode
- Forward All Multicast Traffic
- Forbid IGMP Snooping
- Backpressure
- Broadcast Limit (Pkts/s)
- Detect Remote Faults
- Detection
- Single Fiber
- Minimum Frame Length
- Synchronous status messages
- SSM Code-Type
- Tx DUS/DNU
- Type
- Time (seconds)
- Swap MAC Address
- Source MAC Address
- Destination MAC Address
- PBB Ethertype
- Window Size



Note 1 — Management connectivity between the 5620 SAM and the 7705 SAR may be lost if a line loopback is applied to an Ethernet port that is carrying in-band management traffic. The line loopback remains in effect until the timer expires and the 7705 SAR removes the loopback.

Note 2 — Statistics are collected for IEEE 1588 PTP timestamps only when the Timestamp Capable parameter is enabled on the 7705 SAR-A and 7705 SAR-W. See “Statistics collection overview” and “Viewing statistics” in the *5620 SAM Statistics Management Guide* for more information about how to collect and view statistics.

28 To configure CRC threshold parameters, perform the following steps:

i Remove the check mark from the Disable check box and configure the CRC SD Threshold and CRC SD Threshold Multiplier parameters.

ii Remove the check mark from the Disable check box and configure the CRC SF Threshold and CRC SF Threshold Multiplier parameters.

iii Configure the Window Size (seconds) parameter.

29 If you are configuring an Ethernet port on a 7210 SAS-X, Release 4.0 R1 or later, a 7210 SAS-D or 7210 SAS-M, Release 4.0 R3 or later, or a 7210 SAS-T, the SAP panel is displayed. Perform the following:

i Click on the Select button in the SAP panel. The Select SAP form opens.

ii If required, configure the filter criteria, and click on the Search button.

iii Choose a SAP and click on the OK button. The Select SAP form closes.

30 If you are configuring an Ethernet port on a Release 6.0 R1 or later 2-port ring MDA on a 7705 SAR-8 or 7705 SAR-18, the Vlan Filter panel is displayed.

i Click on the Select button in the Vlan Filter panel. The Select Vlan Filter - Ethernet Port form opens.

ii If required, configure the filter criteria, and click on the Search button.

iii Choose a Vlan Filter and click on the OK button. The Select Vlan Filter - Ethernet Port form closes.

31 If the port is an access or hybrid port with QinQ or dot1q encapsulation, or a network port with dot1q encapsulation, the MEPs tab is displayed. Click on the MEPs tab to add a facility MEP, if required:



Note — Only one facility MEP can be configured on a port.

i Click on the Create button. The MEP (Create) form opens on the General tab.

ii Click on the Select button to choose a global MEG. The Select Maintenance Entity Group form opens.

iii Choose an entry and click on the OK button. The Select Maintenance Entity Group form closes.



Note — For port-based facility MEPs, the Maintenance Domain must be set for a Level of 0 or 1. See Procedure 78-1 for information on creating the MD.

iv Configure the parameters:



Note — Only the parameters that are supported on the NE, daughter card, or port are displayed.

- Auto-Assign ID
- Description
- CCM Messages Enabled
- Priority Level for CCM Messages
- CCM TLV Ignore
- Low-priority Defect
- MAC Address
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)
- CCM Padding Packet Size (Bytes)
- Facility Fault Notify



Note 1 — To enable fault propagation on a LAG facility MEP or on a tunnel facility MEP, the Facility Fault Notify parameter must be enabled.

Note 2 — To link the facility tunnel status to the SAP, the Facility VLAN ID parameter must match the outer encapsulation value of the SAP.

Note 3 — The CCM Padding Packet Size (Bytes) parameter cannot be configured when the CCM interval parameter is set to 10 ms or 100 ms.

v If the MD for the MEP has a Name Type of none the Y.1731 Tests tab is configurable; click on the Y.1731 Tests tab. Otherwise, go to step vii.

vi Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

vii Click on the OK button. A dialog box appears.

viii Click on the OK button. The MEP (Create) form closes.

32 Click on the 802.3ah tab to configure and initiate the 802.3ah EFM OAM diagnostic as described in Procedure 32-42. Otherwise, continue to step 33.

33 Click on the 802.1x Port tab, if required.

34 Configure the parameters:



Note — Only the parameters that are supported on the NE, daughter card, or port are displayed.

- Initialize
- Reauthenticate Control

35 Click on the 802.1x Port Authenticator tab, if required.

36 Configure the parameters:



Note — Only the parameters that are supported on the NE, daughter card, or port are displayed.

- Controlled Port Control
- Quiet Period
- Tx Period
- Supplicant Timeout
- Server Timeout
- Max Req
- Reauth Period
- Reauth Enabled
- Tunneling

You can enable the Tunneling parameter only when:

- the port is in access mode
- the Controlled Port Control parameter is set to Force Authorized
- the port is not used as a SAP (except in an Epipe service)

37 Click on the Select button to choose a RADIUS server policy. The Select Policy - Physical Port form opens.

38 Choose a RADIUS server policy in the list and click on the OK button. The Select Policy - Physical Port form closes and the Physical Port (Edit) form displays the RADIUS policy name.

39 Go to Procedure 16-8 to add a queue group to the port.

40 If the port is an HSMDA access port, the Egress Secondary Shapers tab is present. Click on the Egress Secondary Shapers tab to add an egress secondary shaper to the port, if required, and perform the following steps.



Note 1 — An HSMDA port is initially created with a default egress secondary shaper. The default shaper cannot be deleted, but it can be modified.

Note 2 — Non-default egress secondary shapers can only be created if the port's Mode parameter is not set to the network option.

Note 3 — You cannot switch the Mode of an HSMDA port to network if there are non-default egress secondary shapers on that port. An error message will be issued. You must delete any non-default egress secondary shapers from the port before switching its Mode to network.

i Click on the Create button. The HSMDA Egress Secondary Shaper (Create) form opens, with the General tab displayed.

ii Configure the parameters:

- Name
- Low Burst Max Class
- Rate (Mbps)
- Monitor Threshold (Kbytes)
- Low Burst Limit
- High Burst Increase

  The Rate (Mbps) parameter can only be configured if the associated MAX check box is not enabled.

iii Click on the Classes tab.

iv Configure the Class Rate (kbps), Class Monitor Threshold (Kbytes) and Class Burst Threshold (bytes) parameters for Classes 1 through 8, as required.

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The new entry appears in the list.

41 Click on the LLDP tab, if required. The LLDP configuration form opens with the Nearest Bridge sub-tab displayed.

42 Configure the parameters:

- Administrative Status
- Notifications
- Transmit Management Address
- LLDP TLVs
- Tunneling

43 Repeat step 42 for the Nearest Non TPMR and Nearest Customer sub-tabs under the LLDP tab, as required.

44 Click on the Remote Peers sub-tab under the LLDP tab to search for and display LLDP remote peers associated with the port. These remote peers are used to determine the physical topology of the network.

45 Click on the Qos Pool tab, if required.

46 Choose a QoS pool from the list and click on the Properties button. The QoS Pool (Edit) form opens.

47 Click on the Select button in the Slope Policy panel. The Select Slope Policy - QoS Pool form opens.

48 Choose a slope policy in the list and click on the OK button. The Select Slope Policy- QoS Pool form closes and the QoS Pool (Edit) form reappears with the name of the slope policy.

49 Configure the parameters:

- Reserved CBS (%)
- Default Reserved CBS
- Amber Alarm Action Max (%)
- Amber Alarm Action Step (%)
- Amber Alarm Threshold (%)
- Red Alarm Threshold (%)

50 Click on the OK button. The QoS Pool (Edit) form closes.

51 Perform one of the following:

a Click on the Override Policy Items tab to configure HSMDA overrides. See Procedure 16-10 for more information.

b Continue to step 52.

52 To configure a tunable optic DWDM MDA or IMM on a 7750 SR or 7450 ESS, click on the Optical Transport Channel Unit tab. Otherwise, go to step 67.

53 Configure the following parameters on the General tab:

- FEC Mode
- SF-SD Method
- Configured Data Rate (Gb/s)
- Transmitter Mode
- Transmitter String
- Async Mapping
- Transmitter Bytes
- Expected Rx Mode
- Expected Rx String
- Expected Rx Bytes
- OTU-TIM reaction
- ODU-TIM reaction
- OPU-TIM reaction
- Payload Type (hex)
- Expected Payload Type (hex)
- OPU-PLM reaction
- SF Threshold (1/10E-n bits received)
- SF Threshold Coeff
- SD Threshold (1/10E-n bits received)
- SD Threshold Coeff
- SF Clr Threshold (1/10E-n bits received)
- SF Clr Threshold Coeff
- SD Clr Threshold (1/10E-n bits received)
- SD Clr Threshold

54 Click on the OTU Alarms tab and select the OTU alarms for the Configured Alarms parameter.

55 Click on the Select button in the DWDM panel to choose a channel. The Wave Length Reference - Physical Port form opens.

56 Use the configurable filter and click on the Search button to generate a list of configurable channels and related wavelengths and frequencies.

57 Select a channel and click on the OK button. The Wave Length Reference - Physical Port form closes and the channel number, wavelength, and frequency are displayed in the DWDM panel of the Physical Port (Edit) form.

58 Click on the Optical tab and configure the following parameters on the Wavelength Track tab:

- Wave Tracker Encode
- Wave Tracker Power Control
- Configured Alarms
- Wave Key1
- Wave Key2
- Target Power

59 Click on the Optical Amplifier tab and configure the Configured Alarms parameter.

60 Click on the Optical Tunable Dispersion Compensation Module tab.

61 Configure the following parameters:

- Channel
- Dispersion
- Control Mode
- Configured Alarms

62 Click on the Apply button. A dialog box appears.

63 Click on the Yes button.

64 To configure coherent optics options for a 1-Port 100GE OTU4 DWDM tunable optic IMM on a 7750 SR or 7450 ESS, click on the Coherent Optics tab. Otherwise, go to step 67.

65 Configure the parameters on the Coherent Optical Module tab:

- Coherent Optical Channel
- Dispersion Control Mode
- Dispersion
- Dispersion Sweep Start
- Dispersion Sweep End
- Tx Target Power
- Rx LOS Threshold
- Rx LOS Reaction
- Carrier Phase Recovery
- Configured Alarms

66 Click on the Operational Status tab to view information about the state of the optical port.

67 Click on the other tabs to view and edit additional port information.

68 Click on the OK button. The Physical Port (Edit) form closes.

Procedure 16-2 To change the port mode

Perform this procedure to change the port mode between Network, Access, and Hybrid modes.



Note — Save the device configuration before you perform this procedure. See the appropriate NE documentation for more information.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the port object where you want to change the port mode. The path is Network→*NE*→Shelf→Card Slot *n*→Daughter Card Slot *n*→Port *n*/*n*/*n*.

3 Right-click on the Port icon and choose Properties. The Physical Port (Edit) form opens with the General tab displayed.

4 Change the Mode parameter as required and click on the Apply button.

5 If you are changing the mode from Access to Network and services are configured on the port, warnings are displayed in a dialog box, depending on the permissions that are associated with your user role. Perform one of the following:

a The default warning dialog indicates that the object has dependencies that will be deleted if you apply the port mode change.

i Click on View Dependencies button to see the number of dependencies (services and interfaces) associated with the port.

ii Click on the OK button.

iii Confirm that you understand the implications of changing the port mode by enabling the "I understand the implications of this action" check box. A confirmation dialog box appears.

iv Click on the Yes button. Any services and interfaces associated with the port, including SAPs, are deleted, and the mode for the port is changed to Network.



Note — Changing the port mode from Access to Network without first removing the dependencies results in a TopologyMisconfigured alarm.

b For users who have the port.RestrictNodeConfigModify permission associated with their role, a warning form appears, indicating that the object has dependencies that must be removed before proceeding.

i Click on View Dependencies button to see the number of dependencies (services and interfaces) associated with the port.

ii Click on the OK button.

iii Remove the services or interfaces associated with the port. You can manually delete them or move them to other ports as described in this chapter.

iv Repeat steps 3 and 4 to change the port mode to Network.

Procedure 16-3 To migrate SAPs from access mode to hybrid mode

Perform this procedure on Ethernet or SC-LAG access ports that contain SAPs.



Note — Save the device configuration before you perform this procedure. See the appropriate NE documentation for more information.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the port object where you want to migrate SAPs. The path is Network→*NE*→Shelf→Card Slot *n*→Daughter Card Slot *n*→Port *n*/*n*/*n*.

3 Right-click on an Ethernet port or SC-LAG port icon and choose Properties. The Physical Port (Edit) form opens with the General tab displayed.

4 Change the Mode parameter from Access to Hybrid. A dialog box opens.

5 Click on the Yes button. A warning form appears.

6 Perform an admin save.

7 Select the I understand the implications of this action check box and click on the Yes button. The SAP Migration Result form displays information about the number of SAPs migrated.

8 Click on the OK button to close the forms.

Procedure 16-4 To configure the 5620 SAM to retain non-default port MTU values

Perform this procedure to configure the 5620 SAM server for non-default MTU refresh behavior.

The MTU value for a port is associated with the port mode, such as access or network, and the port encapsulation type. If you change the mode or encapsulation type of a port, the MTU value changes to the associated default. If you do not want the port MTU values to change, you can use this procedure to configure the 5620 SAM to retain each port MTU value, regardless of a mode or encapsulation type change.



Note — You must perform this procedure on each main server in a redundant 5620 SAM deployment.

1 Log in to the 5620 SAM main server station as the samadmin user.

2 Navigate to the 5620 SAM server configuration directory, typically /opt/5620sam/server/nms/config.

3 Open the nms-server.xml file with a plain-text editor.



Caution — Contact your Alcatel-Lucent technical support representative before you attempt to modify the nms-server.xml file. Modifying the nms-server.xml file can have serious consequences that can include service disruption.

4 Add the following line to the end of the file:

```
<customMTURefresh refresh="true"/>
```

5 Save and close the nms-server.xml file.

6 Open a console window.

7 Navigate to the 5620 SAM server binary directory, typically /opt/5620sam/server/nms/bin.

8 If the main server is a standalone server, or the primary server in a redundant deployment, enter the following:

```
bash$ ./nmsserver.bash read_config ↵
```

The main server reads the nms-server.xml file and puts the configuration change into effect.

9 If the main server is the standby server in a redundant deployment, enter the following:

```
bash$ ./nmsserver.bash force_restart ↵
```

The main server restarts and puts the configuration change into effect.

10 Close the console window.

Procedure 16-5 To copy or move L2 SAPs between ports

You can also use the 5620 SAM clipboard to copy or move SAPs. See chapter 3 for information about using the 5620 SAM clipboard.

1 For the source NE, disable automatic configuration backup if enabled in the backup policy assigned to the NE, by configuring the Auto Backup Scheme parameter appropriately. See "NE maintenance overview" in the *5620 SAM System Administrator Guide* for information about configuring automatic configuration backup for an NE.

2 On the source NE, use a CLI to back up the device configuration to a file. Ensure that you use a unique name for the backup file to ensure that it is not accidentally overwritten. Enter the following at the CLI prompt:

admin save *file_name* ↵

where *file_name* is a name that differs from the existing configuration file names on the NE and identifies this as the configuration in effect before the copy or move operation



Caution — An unsuccessful SAP copy or move may result in the deletion of one or more source SAPs from the source NE. The backed-up configuration file is required to restore the configuration on the source NE if a SAP copy or move operation fails.

See the appropriate device documentation for more information about saving the device configuration to a file.

3 For the destination NE, disable automatic configuration backup if enabled in the backup policy assigned to the NE by configuring the Auto Backup Scheme parameter appropriately. See "NE maintenance overview" in the *5620 SAM System Administrator Guide* for more information about configuring automatic configuration backup for an NE.

4 On the destination NE, use a CLI to back up the device configuration to a file. Ensure that you use a unique name for the backup file to ensure that it is not accidentally overwritten. Enter the following at the CLI prompt:

admin save *file_name* ↵

where *file_name* is a name that differs from the existing configuration file names on the NE and identifies this as the configuration in effect before the copy or move operation

See the appropriate device documentation for more information about saving the device configuration to a file.

5 Open the Deployment form to monitor deployments as they occur during the SAP copy or move operation. Choose Administration→NE Maintenance→Deployment from the 5620 SAM main menu. The Incomplete Deployments tab is displayed.



Caution — Alcatel-Lucent strongly recommends that you monitor the NE deployments and the alarm window during a SAP copy or move operation to ensure that faults that may arise during the operation are immediately detected.

The Incomplete Deployments tab of the Deployment form notifies the 5620 SAM operator of configuration changes that are not successfully deployed to the NE, and the 5620 SAM alarm window alerts the operator to object failures on the NE that are related to the copy or move operation.

6 Choose Tools→Copy/Move SAPs. The Copy/Move SAPs form opens with the General tab displayed.

7 Arrange the forms on the GUI so that the Copy/Move SAPs form, the Deployment form, and the alarm window are all shown.

8 Click on the Result Export Path tab. The Result Export Path form opens.

9 Specify the file name and location in which to save a text file that contains the results of the SAP copy or move operation.

10 Click on the Set button. The Result Export Path form closes.

11 Click on the Select button beside the Source Node parameter. The Select Network Elements form opens.

12 Choose a source NE from the list and click on the OK button. The Select Network Elements form closes and the NE identifier is displayed in the Source panel.

13 Click on the Select button beside the Source Port parameter. The Select Port form opens.

14 Configure the filter criteria. A list of available ports is displayed.

15 Select a port in the list and click on the OK button. The Select Port form closes and the port identifier is displayed in the Source panel.

16 Click on the Select button beside the Destination Node parameter. The Select Network Elements form opens.

17 Select a destination NE in the list and click on the OK button. The Select Network Elements form closes and the NE identifier is displayed in the Destination panel.

18 Click on the Select button beside the Destination Port parameter. The Select Port form opens.

19 Configure the filter criteria. A list of available ports is displayed.

20 Select a port in the list and click on the OK button. The Select Port form closes and the port identifier is displayed in the Destination panel.

21 Configure the parameters:

- Current Mode
- Outer Encap Value Start
- Outer Encap Value End
- Inner Encap Value Start
- Inner Encap Value End
- Service Type
- Outer Encap Value Offset
- Inner Encap Value Offset
- Action Type
- Continue on individual Failure

22 Click on the Execute button to begin the copy or move operation. The Execution Result panel displays the execution state of the copy or move operation and the number of successful and failed operations based on the input criteria.



Note — When you copy or move a SAP on an L2 interface and there is a non-zero value assigned to the PIM Snooping parameter Maximum Number of Groups, the value is not copied or moved to the new location. You must manually configure the Maximum Number of Groups parameter in the new location.

23 Monitor the Deployments form and the alarm window for any deployment failures and faults related to the SAP copy or move operation. Click on the Refresh button of the Deployments form to update the list, if required.

24 Click on the Result tab to view a list of the successful and failed operations as identified by the 5620 SAM.

25 Click on the Refresh Result button to view the most recent results.

26 To view the information for an individual SAP copy or move operation, move the mouse pointer over the Message field of the operation.

27 If a copy or move operation fails, you can restore the previous source NE configuration using the backup configuration file created in step 2. To restore the previous NE configuration:

i Open a CLI on the source NE.

ii Enter the following at the command prompt to load the saved configuration file:

```
exec file_name ↵
```

where *file_name* is the name of the configuration file that was specified in step 2

The SAPs that were deleted during the unsuccessful copy or move operation are restored on the NE.

iii Enter the following at the command prompt to save the NE configuration:

```
admin save ↵
```

28 If a copy or move operation partially fails, you can restore the previous destination NE configuration using one of the following methods.



Note — If the copy or move operation fails completely, there is no need to restore the previous configuration because no SAPs are created on the destination NE.

a Restore the backed-up configuration file.

i Open a CLI on the destination NE.

ii Enter the following at the command prompt to load the saved configuration file:

exec *file_name* ↵

where *file_name* is the name of the configuration file specified in step 4

The previous configuration is restored on the NE.

iii Enter the following at the command prompt to save the NE configuration:

admin save ↵

b Manually delete the SAPs that the copy or move operation created on the destination NE.

29 Restore the previous automatic configuration backup functionality in the backup policy used by the source NE, if required, by configuring the Auto Backup Scheme parameter appropriately. See “NE maintenance overview” in the *5620 SAM System Administrator Guide* for information about configuring automatic configuration backup for an NE.

30 Restore the previous automatic configuration backup functionality in the backup policy used by the destination NE, if required, by configuring the Auto Backup Scheme parameter appropriately. See “NE maintenance overview” in the *5620 SAM System Administrator Guide* for information about configuring automatic configuration backup for an NE.

31 Close the Copy/Move SAPs and the Deployments forms.

Procedure 16-6 To move L3 SAPs within or between ports on the same NE

Perform this procedure to move one or more L3 access interface SAPs within a port, or from one port to another port on the same NE.

To copy or move L3 access interface SAPs from one port to another on different NEs, see “XML API template administration” in the *5620 SAM Scripts and Templates Developer Guide* for information about the administrative tasks associated with service templates.

You can also use the 5620 SAM clipboard functionality to move SAPs. See chapter 3 for information about using the 5620 SAM clipboard.



Note — L3 access interfaces are not bound to a port; for example, loopback interfaces cannot be moved.

1 For the NE, disable automatic configuration backup if enabled in the backup policy assigned to the NE, by configuring the Auto Backup Scheme parameter appropriately. See "NE maintenance overview" in the *5620 SAM System Administrator Guide* for information about configuring automatic configuration backup for an NE.

2 On the NE, use a CLI to back up the device configuration to a file. Ensure that you use a unique name for the backup file to ensure that it is not accidentally overwritten. Enter the following at the CLI prompt:

admin save *file_name* ↵

where *file_name* is a name that differs from the existing configuration file names on the NE and identifies this as the configuration in effect before the move operation

See the appropriate device documentation for more information about saving the device configuration to a file.

3 Open the Deployment form to monitor deployments as they occur during the SAP move operation. Choose Administration→NE Maintenance→Deployment from the 5620 SAM main menu. The Incomplete Deployments tab is displayed.



Caution — Alcatel-Lucent strongly recommends that you monitor the NE deployments and the alarm window during a SAP move operation to ensure that faults that may arise during the operation are immediately detected.

The Incomplete Deployments tab of the Deployment form notifies the 5620 SAM operator of configuration changes that are not successfully deployed to the NE, and the 5620 SAM alarm window alerts the operator to object failures on the NE that are related to the move operation.

4 Choose Tools→Copy/Move SAPs. The Copy/Move SAPs form opens with the General tab displayed.

5 Arrange the forms on the GUI so that the Copy/Move SAPs form, the Deployment form, and the alarm window are all shown.

6 Click on the Result Export Path tab. The Result Export Path form opens.

7 Specify the file name and location in which to save a text file that contains the results of the SAP move operation.

8 Click on the Set button. The Result Export Path form closes.

9 Click on the Select button beside the Source Node parameter. The Select Network Elements form opens.

10 Choose an NE from the list and click on the OK button. The Select Network Elements form closes and the NE identifier is displayed in the Source panel.

11 Click on the Select button beside the Source Port parameter. The Select Port form opens.

12 Configure the filter criteria. A list of available ports is displayed.

13 Choose a port in the list and click on the OK button. The Select Port form closes and the port identifier is displayed in the Source panel.

14 Click on the Select button beside the Destination Port parameter. The Select Port form opens.

15 Configure the filter criteria. A list of available ports is displayed.

16 Select a port in the list and click on the OK button. The Select Port form closes and the port identifier is displayed in the Destination panel.

17 Configure the parameters:

- Current Mode
- Outer Encap Value Start
- Outer Encap Value End
- Inner Encap Value Start
- Inner Encap Value End
- Service Type
- Outer Encap Value Offset
- Inner Encap Value Offset
- Continue on individual Failure

18 Click on the Execute button to start the move operation. The Execution Result panel displays the execution state of the move operation and the number of successful and failed operations based on the input criteria.

19 Monitor the Deployments form and the alarm window for any deployment failures and faults related to the SAP move operation. Click on the Refresh button of the Deployments form to update the list, if required.

20 Click on the Result tab to view a list of the successful and failed operations as identified by the 5620 SAM.

21 Click on the Refresh Result button to view the most recent results.

22 To view the information for an individual SAP move operation, move the mouse pointer over the Message field of the operation.

23 If a move operation fails, you can restore the previous NE configuration using the backup configuration file created in step 2. To restore the previous NE configuration:

i Open a CLI on the NE.

ii Enter the following at the command prompt to load the saved configuration file:

exec *file_name* ↵

where *file_name* is the name of the configuration file specified in step 2

The SAPs that were deleted during the unsuccessful move operation are restored on the NE.

iii Enter the following at the command prompt to save the NE configuration:

```
admin save ↵
```

24 Restore the previous automatic configuration backup functionality in the backup policy used by the NE, if required, by configuring the Auto Backup Scheme parameter appropriately. See "NE maintenance overview" in the *5620 SAM System Administrator Guide* for information about configuring automatic configuration backup for an NE.

25 Close the Copy/Move SAPs and the Deployments forms.

Procedure 16-7 To move L3 subscriber interface SAPs between ports on the same NE

Perform this procedure to move one or more L3 subscriber interface SAPs from one port to another port on the same NE.

To copy or move L3 subscriber interface SAPs from one port to another on different NEs, see "XML API template administration" in the *5620 SAM Scripts and Templates Developer Guide* for more information about the administrative tasks associated with service templates.

You can also use the 5620 SAM clipboard functionality to move SAPs. However, you can only move all of the SAPs in a group interface; you cannot be used to move a subset of SAPs. See chapter 3 for information about using the 5620 SAM clipboard.

1 For the NE, disable automatic configuration backup if enabled in the backup policy assigned to the NE, by configuring the Auto Backup Scheme parameter appropriately. See "NE maintenance overview" in the *5620 SAM System Administrator Guide* for information about configuring automatic configuration backup for an NE.

2 On the NE, use a CLI to back up the device configuration to a file. Ensure that you use a unique name for the backup file to ensure that it is not accidentally overwritten. Enter the following at the CLI prompt:

```
admin save file_name ↵
```

where *file_name* is a name that differs from the existing configuration file names on the NE and identifies this as the configuration in effect before the move operation

See the appropriate device documentation for more information about saving the device configuration to a file.

3 Open the Deployment form to monitor deployments as they occur during the SAP move operation. Choose Administration→NE Maintenance→Deployment from the 5620 SAM main menu. The Incomplete Deployments tab is displayed.



Caution — Alcatel-Lucent strongly recommends that you monitor the NE deployments and the alarm window during a SAP move operation to ensure that any faults that arise during the operation are immediately detected.

The Incomplete Deployments tab of the Deployment form notifies the 5620 SAM operator of configuration changes that are not successfully deployed to the NE, and the 5620 SAM alarm window alerts the operator to object failures on the NE that are related to the move operation.

4 Choose Tools→Copy/Move SAPs. The Copy/Move SAPs form opens with the General tab displayed.

5 Arrange the forms on the GUI so that you can view the entire Copy/Move SAPs form, the Deployment form, and the alarm window.

6 Click on the Result Export Path tab. The Result Export Path form opens.

7 Specify the file name and location in which to save a text file that contains the results of the SAP move operation.

8 Click on the Set button. The Result Export Path form closes.

9 Click on the Select button beside the Source Node parameter. The Select Network Elements form opens.

10 Choose an NE from the list and click on the OK button. The Select Network Elements form closes and the NE identifier is displayed in the Source panel.

11 Click on the Select button beside the Source Port parameter. The Select Port form opens.

12 Configure the filter criteria. A list of available ports is displayed.

13 Choose a port in the list and click on the OK button. The Select Port form closes and the port identifier is displayed in the Source panel.

14 Configure the filter criteria. A list of available ports is displayed.

15 Choose a port in the list and click on the OK button. The Select Port form closes and the port identifier is displayed in the Destination panel.

16 Configure the parameters:

- Current Mode
- Service Type
- Outer Encap Value Offset
- Inner Encap Value Offset
- Continue on individual Failure

17 Click on the Execute button to start the move operation. The Execution Result panel displays the state of the move operation, and the number of successful and failed operations based on the input criteria.

18 Monitor the Deployments form and the alarm window for any deployment failures and faults related to the SAP move operation. Click on the Refresh button of the Deployments form to update the list, if required.

19 Click on the Result tab to view a list of the successful and failed operations, as identified by the 5620 SAM.

20 Click on the Refresh Result button to view the most recent results.



Note — If one SAP fails, all SAPs under the same group interface fail because the SAPs can only move together. In this case, there is insufficient information to determine which SAP caused the problem using the 5620 SAM.

21 To view information about an individual SAP move operation, move the mouse pointer over the Message field of the operation.

22 If a move operation fails, you can restore the previous NE configuration using the backup configuration file created in step 2. To restore the previous NE configuration:

i Open a CLI on the source NE.

ii Enter the following at the command prompt to load the saved configuration file:

exec *file_name* ↵

where *file_name* is the name of the configuration file specified in step 2

The SAPs that were deleted during the unsuccessful move operation are restored on the NE.

iii Enter the following at the command prompt to save the NE configuration:

admin save ↵

23 Restore the previous automatic configuration backup functionality in the backup policy used by the NE, if required, by configuring the Auto Backup Scheme parameter appropriately. See "NE maintenance overview" in the *5620 SAM System Administrator Guide* for information about configuring automatic configuration backup for an NE.

24 Close the Copy/Move SAPs and the Deployments forms.

Procedure 16-8 To add a queue group to an Ethernet port

You can create a port queue group on an Ethernet port after creating an Ingress/Egress Queue Group Template policy.



Note — You must use the same name for the port queue group and Ingress/Egress Queue Group Template policy.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the port object where you want to add a queue group. The path is Network→*NE*→Shelf→Card Slot *n*→Daughter Card Slot *n*→Port *n*/*n*/*n*.

3 Right-click on an Ethernet port icon and choose Properties. The Physical Port (Edit) form opens with the General tab displayed.

4 Click on the Ethernet tab.

5 Perform one of the following:

- **a** Click on the Network Egress Queue Group tab.
- **b** Click on the Access Egress Queue Group tab.
- **c** Click on the Access Ingress Queue Group tab.



Note — The Network Egress Queue Group tab is available if queue groups are supported on the port, depending on the NE release and IOM type. See section "Port queue groups" in chapter 62 for more information about supported devices and IOM types.

6 Click on the Create button. The Queue Group (Create) form opens with the General tab displayed.

7 Click on the Select button in the Queue Group Template Policy panel. The Select Queue Group Template Policy list form opens.

8 Choose a queue group template policy from the list and click on the OK button. The Select Queue Group Template Policy list form closes.

9 Configure the parameters:

- Instance ID
- Description

10 If you are adding a network egress queue group, go to step 11. Otherwise, continue to step 13.

11 Click on the Select button in the Policer Control Policy panel to select a policer control policy. The Select Policer Control Policy list form opens.

12 Choose a policer control policy from the list and click on the OK button. The Select Policer Control Policy list form closes and the Network Egress Queue Group (Create) form refreshes with the Policer Control Policy information.

13 Click on the Select button in the Accounting Policy panel to select an accounting policy. The Select Accounting Policy list form opens.



Note — Only the accounting policies with the Type parameter configured to one of the following options are listed:

- Queue Group Octets
- Queue Group Packets
- Combined Queue Group

14 Choose an accounting policy from the list and click on the Ok button. The Select Accounting Policy list form closes and the Queue Group (Create) form refreshes with the accounting policy information.

15 Configure the Collect Accounting Statistics parameter.

16 Click on the Select button in the Scheduler Policy panel to assign a scheduler policy to the port. The Select Scheduler Policy list form opens.

17 Choose a scheduler policy from the list and click on the OK button. The Select Scheduler Policy list form closes.

18 If you are adding an access ingress queue group, go to step 25. Otherwise, continue to step 19.

19 Configure the parameters:

- Aggregate Rate Limit (kbps)
- Frame-Based Accounting

The Aggregate Rate Limit (kbps) and Frame-Based Accounting parameters are configurable only if you did not select a scheduler policy in step 17.
The Frame-Based Accounting parameter is configurable only if you configure the Aggregate Rate Limit (kbps) parameter.

20 If you are adding a network egress queue group (including queue groups for HSMDA), go to step 25. Otherwise, continue to step 21.

21 Click on the Host Matching tab.



Note — The Host Matching tab will only be available if the Instance ID is set to 1.

22 Click on the Create button. The Host String (Create) form opens.

23 Configure the Host String parameter.

24 Click OK. The Host String (Create) form closes and the information on the Host Matching tab is updated.

25 Click on the Overrides: Type Queue tab, where Type will be Network Egress, Access Egress, or Access Ingress, depending on your selection in step 5.

26 Click on the Create button. The Queue Override (Create) form opens.

27 Click on the Select button to choose a Queue ID. The Select Queue - Queue Override list form opens.

28 Choose an entry from the list and click on the OK button. The Select Queue - Queue Override list form closes and the Queue Override (Create) form refreshes with the queue information.

29 Click on the Override tab.

30 If you are configuring an access egress queue group queue override for HSMDA, then go to step 33.

31 Configure the parameters:

- Committed Burst Size (kb)
- Maximum Burst Size (bytes)
- High Priority Reserved
- PIR Adaptation
- CIR Adaptation
- PIR (kbps)
- CIR (kbps)
- Weight
- CIR Weight

The Weight and CIR Weight parameters are only applicable to access egress queue group overrides.

The parameters are configurable when the Override check box is enabled.

32 Go to step 36.

33 Configure the parameters as required:

- PIR (kbps)
- MBS (bytes)
- WRR Weight

The parameters are configurable when the associated Override check box is enabled.

34 If you need to configure an override for a Slope Policy, then enable the associated Override check box and click the Select button.The Select Slope Policy form opens.

35 Select the required Slope Policy and click OK. The Select Slope Policy form closes and the Queue Override (Create) form refreshes with the Slope Policy information.

36 Click on the OK button to save the configuration and close the Queue Override (Create) form. A dialog box appears.

37 Click on the OK button.

38 Click on the OK button to save the configuration and close the Queue Group (Create) form. A dialog box appears.

39 Click on the OK button. A dialog box appears.

40 Click on the Yes button to save the configuration and close the Physical Port (Edit) form.

41 Close the Network Element (Edit) form.

Procedure 16-9 To configure SONET ports

Perform the steps in this procedure as required depending on the daughter card and port type that you are configuring.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the port object where you want to configure a SONET port. The path is Network→*NE*→Shelf→Card Slot *n*→Daughter Card Slot *n*→Port *n*/*n*/*n*.

3 Right-click on a port icon and choose Properties. The Physical Port (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- Description
- Speed
- DDM Event Suppression
- Current OLC State

The DDM Event Suppression parameter is configurable only on ports on SFPs and XFPs optical modular transceivers.

5 Click on the States tab.

6 Configure the Administrative State parameter.

7 Click on the Channels tab to configure the SONET/SDH channel.

a Click on the Create button to create a new channel.

b Choose a channel from the list and click on the Properties button to view and edit the channel parameters.

c Choose a channel from the list and click on the Delete button to remove a channel from the port.

8 Click on the SONET tab.

9 Configure the parameters:

- Framing
- Clock Source
- Loopback
- Single Fiber
- Hold Time Down (100s of ms)
- Hold Time Up (100s of ms)
- Tx DUS/DNU

10 Click on the SONET Monitoring tab.

11 Configure the parameters:

- BER Signal Degradation Threshold
- BER Signal Failure Threshold
- Report Alarms

12 Click on the SONET Overhead tab.

13 Configure the parameters:

- SONET Section Trace Mode
- J0 Byte

  Enter a J0 byte that identifies the circuit. This byte is inserted continuously at source. This can be checked against the expected value by the receiver. If no byte is entered, then null is used. The parameter is configurable when the SONET Section Trace Mode is set to Byte.
- J0 String

  The parameter is configurable when the SONET Section Trace Mode is set to String.

14 Click on the other tabs in the properties form to view and edit additional port information.

15 Click on the OK button. The Physical Port (Edit) form closes.

Procedure 16-10 To configure an HSMDA override

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure an HSMDA override and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon to the HSMDA card level.

4 Expand the port level and click on a port object. The Physical Port (Edit) form opens with the General tab displayed.

5 Click on the Override Policy Items tab. The Override configuration form opens with the HSMDA Scheduler tab displayed.

6 Click on the Create button. The Port Egress HSMDA Scheduler Policy Override (Create) form opens with the General tab displayed.

7 Click on the Override tab.

8 Configure the parameters:

- Maximum Rate (Mbps)
- Rate (Mbps)
- Weight in Group

The Rate (Mbps) parameter is configurable when a Group is not specified for the applied HSMDA scheduler policy. The Weight in Group parameter is only configurable when Group 1 or Group 2 is specified for the HSMDA scheduler policy.

9 Click on the OK button. A dialog box appears.

10 Click on the OK button. The Override configuration form is updated with the scheduler override.

11 Close the Physical Port (Edit) form.

Procedure 16-11 To configure TDM DS3 ports

Perform the steps in this procedure as required depending on the port type that you are configuring.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the port object where you want to configure a TDM DS3 port. The path is Network→*NE*→Shelf→Card Slot *n*→Daughter Card Slot *n*→Port *n*/*n*/*n*.

3 Right-click on a port icon and choose Properties. The Physical Port (Edit) form opens with the General tab displayed.

4 Configure the General tab parameters:

- Description
- Speed
- Current OLC State
- DDM Event Suppression

5 Click on the States tab.

6 Configure the Administrative State parameter.

7 Click on the DS3/E3 tab.

8 Configure the parameters:

- Line Buildout
- Type

9 Click on the other tabs in the properties form to view and edit additional port information.

10 Click on the OK button. The Physical Port (Edit) form closes.

Procedure 16-12 To configure serial ports

Perform this procedure to configure a port on a 12 × Serial Data card on the 7705 SAR.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the port object where you want to configure a serial port. The path is Network→*NE*→Shelf→Card Slot *n*→Daughter Card Slot *n*→Port *n*/*n*/*n*.

3 Right-click on a port icon and choose Properties. The Physical Port (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- Description
- Speed
- Serial Type
- Current OLC State
- Revert OLC State

5 Click on the States tab.

6 Configure the Administrative State parameter.

7 Click on the other tabs in the properties form to view and edit additional port information.

8 Click on the OK button. The Physical Port (Edit) form closes.

Procedure 16-13 To configure PW ports

Perform this procedure to configure a pseudo-wire port on an NE.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on an NE and choose Properties. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the PW Ports tab. A list of existing PW ports is displayed.

4 Click on the Create button. The PW Port (Create) form opens.

5 Configure the parameters:

- PW Port ID
- Auto-Assign ID
- Encapsulation Type

6 Configure node redundancy for the PW port, if required.

i Click on the Node Redundancy button. The Manage Node Redundancy form appears, preconfigured for MC peer groups.

ii Click on the Search button and configure an existing MC peer group, or click on the Create button and configure a new MC peer group (see Procedure 36-1.

The Node Redundancy button allows you to access the MC sync group configuration within the MC peer group in order to add PW port sync tags.

7 Click on the OK button. The PW Port (Create) form closes and a dialog box appears.

8 Click on the OK button. The dialog box closes and the Network Element (Edit) form reappears with the new PW port listed.

9 Click on the Apply button. A dialog box appears.

10 Click on the Yes button. The dialog box and the Network Element (Edit) form close.

Procedure 16-14 To configure a 7210 SAS-M channelized TDM DS1 or E1 port

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the port object where you want to configure a 7210 SAS-M channelized TDM DS1 or E1 port. The path is Network→*NE*→Shelf→Card Slot *n*→Daughter Card Slot *n*→Port *n*/*n*/*n*.

3 Right-click on a 7210 SAS-M port object that contains a channelized DS1 or E1 and choose Properties. The Physical Port (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- Description
- Current OLC State

5 Click on the Select button in the Split Horizon Group panel. The Select Split Horizon Group - Physical Port form opens.

6 Choose an SHG and click on the OK button. The Select Split Horizon Group - Physical Port form closes and the Physical Port (Edit) form refreshes with the SHG name.

Note — To create or delete a 7210 SAS SHG, see Procedure 16-16.

7 Click on the DS1/E1 tab.

8 Configure the parameters:

- Port Type
- Line Length
- Line Impedance

Note — The Line Impedance parameter only appears when the Port Type parameter is set to E1.

9 Click on the QoS Pool tab.

10 Choose a QoS pool from the list and click on the Properties button. The QoS Pool (Edit) form opens.

11 Click on the Select button in the Slope Policy panel. The Select Slope Policy - QoS Pool form opens.

12 Choose a slope policy in the list and click on the OK button. The Select Slope Policy - QoS Pool form closes and the QoS Pool (Edit) form refreshes with the name of the slope policy.

13 Click on the OK button. The QoS Pool (Edit) form closes.

14 Click on the States tab.

15 Configure the Administrative State parameter.

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The Physical Port (Edit) form closes.

Procedure 16-15 To assign policies to a 7210 SAS Ethernet port

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to a configured Ethernet port object on a 7210 SAS device. The path is Network→*NE*→Shelf→Card Slot *n*→Daughter Card Slot *n*→Port *n*/*n*/*n*.

3 Right-click on a configured Ethernet port object and choose Properties. The Physical Port (Edit) form opens with the General tab displayed.

4 Click on the Policies tab. The Policies form opens with the General tab displayed.

5 Perform one of the following to assign policies to a 7210 SAS Ethernet port.

- **a** If the port is in access or hybrid mode, go to step 6.
- **b** If the port is in network mode or is an L2Uplink port, go to step 7.

6 You can assign port scheduler and access egress policies to 7210 SAS ports in access mode.

- **i** Click on the 7210 Specific tab.
- **ii** Click on the Clear button in the PortScheduler Policy panel to remove the selected policy.
- **iii** Click on the Select button in the PortScheduler Policy panel to assign a port scheduler policy to the port. The Select PortScheduler Policy - Sas Port form opens.
- **iv** Choose a policy from the list and click on the OK button. The Select PortScheduler Policy - Sas Port form closes.
- **v** Click on the Clear button in the Access Egress Policy panel to remove the selected policy.
- **vi** Click on the Select button in the Access Egress Policy panel to assign an access egress policy to the port. The Select Access Egress Policy - Sas Port form opens.
- **vii** Choose a policy from the list and click on the OK button. The Select Access Egress Policy - Sas Port form closes.
- **viii** If the port is in access mode, go to step 8.

7 You can assign accounting, port scheduler, network, and network queue policies when the 7210 SAS port mode is network or hybrid or when it is an L2Uplink port.

- **i** Click on the 7210 Specific tab.
- **ii** Click on the Clear button in the PortScheduler Policy panel to remove the selected policy.
- **iii** Click on the Select button in the PortScheduler Policy panel to assign a port scheduler policy to the port. The Select PortScheduler Policy - Sas Port form opens.
- **iv** Choose a policy from the list and click on the OK button. The Select PortScheduler Policy - Sas Port form closes.
- **v** Click on the Clear button in the Network Policy panel to remove the selected policy.
- **vi** Click on the Select button in the Network Policy panel to assign a network policy to the port. The Select Network Policy - Sas Port form opens.

vii Choose a policy from the list and click on the OK button. The Select Network Policy - Sas Port form closes.

viii Click on the Clear button in the Network Queue panel to remove the selected policy.

ix Click on the Select button in the Network Queue panel to assign a network queue policy to the port. The Select Network Queue Policy - Physical Port form opens.

x Choose a policy from the list and click on the OK button. The Select Network Queue Policy - Physical Port form closes.

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button to apply the changes. The Physical Port (Edit) form closes.

10 Close the Network Element (Edit) form.

Procedure 16-16 To create a 7210 SAS SHG

Traffic that arrives on a access or access uplink port or LAG within an SHG is not copied to other ports and LAGs in the same SHG; the traffic is copied to ports and LAGs in other SHGs if they exist within the same VPLS. Ports and LAGs are added to an SHG when you configure a port or LAG on a 7210 SAS. SHGs are not supported for a VPLS instance.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure the SHG and select Properties. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Split Horizon Groups tab.

4 Click on the Create button. The Split Horizon Group (Create) form opens.

5 Configure the parameters:

- Name
- Description

6 Click on the OK button. A dialog box appears.

7 Click on the OK button. The SHG is added to the displayed list.



Note 1 — Only one SHG can be configured per service.

Note 2 — A SHG and a Mesh SDP Binding cannot exist simultaneously on a single service.

8 Repeat steps 4 to 7 to add another SHG, if required.

9 To view the ports, LAGs, and faults that are associated with an SHG, choose an SHG from the list and click on the Properties button.

10 If you need to delete an SHG, select the SHG and click on the Delete button. A dialog box appears.

11 Enable the check box and click on the Yes button. You cannot delete an SHG if there are any ports or LAGs bound to it.

12 Close the Network Element (Edit) form.

Procedure 16-17 To configure a virtual Ethernet port on a 7705 SAR 2-port ring MDA

Perform this procedure to configure a virtual Ethernet port on a 7705 SAR 2 × 10-Gig Bridged Ethernet XFP + 1 × 2.5G Virtual Ethernet card on a 7705 SAR-8 and 7705 SAR-18, Release 6.0 R1 or later. See Procedure 43-6 for information about configuring a network policy of ring type for a 7705 SAR. See Procedure 15-33 for information about configuring a ring port on a 7705 SAR 2 × 10-Gig Bridged Ethernet XFP + 1 × 2.5G Virtual Ethernet card.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Choose Network→*NE*→Shelf→Card Slot *n*→Daughter Card Slot *n*→Virtual Port *n*/*n*/*n*, where the virtual port is the port object you need to configure.

3 Right-click on the Virtual Port icon and choose Properties. The Virtual Port (Edit) form opens with the General tab displayed.

4 Configure the parameters:



Note — Only the parameters that are supported on the NE, daughter card, or port are displayed.

- Description
- Configured MAC
- Mode
- Encapsulation Type
- MTU (bytes)
- DDM Event Suppression
- Load Balance Algorithm
- Current OLC State
- Revert OLC State

5 Click on the States tab.

6 Configure the Administrative State parameter.

7 Click on the Policies tab. The Policies form opens with the General tab displayed.

8 Click on the Select button in the Network Queue panel and select a network queue policy from the list.

9 Click on the OK button. The network queue policy appears in the Network Queue panel.

10 Click on the Ethernet tab. The Ethernet form opens with the General tab displayed.

11 Configure the parameters:



Note — Only the parameters that are supported on the NE, daughter card, or port are displayed.

- Down When Looped
- Egress Scheduler Mode
- CFM Loopback Mode
- Keep Alive Interval (Sec)
- Retry Timeout (Sec)
- No Retry
- Use Broadcast Address
- Egress Rate (Kbps)
- Type
- Time (seconds)

You must configure the Down When Looped parameter value as Enabled to see the Down When Looped Configuration panel parameters.

12 Click on the Network Interfaces tab to create a network interface on the virtual Ethernet port.

13 Click on the Add button. The Create Network Interface - Routing Instance form opens. Perform steps 4 to 49 of Procedure 22-9 to create a network interface.



Note — You can only bind a virtual Ethernet port to a network interface.

14 Click on the other tabs in the properties form to view additional virtual port information such as physical links, statistics, and faults.

15 Click on the Apply button. A dialog box appears.

16 Click on the Yes button.

17 Click on the OK button. The Virtual Port (Edit) form closes.

Procedure 16-18 To configure PoE ports on a 7210 SAS-T ETR

The 7210 SAS-T ETR supports PoE and PoE Plus on ports 19 through 22. See the *7210 SAS M, T, and X Interface Configuration Guide* for more information about 7210 SAS-T ETR support of PoE.

Perform this procedure to configure PoE on applicable Ethernet ports or to view PoE connection information.



Note 1 — For 7210 SAS devices, only the 7210 SAS-T ETR chassis variant supports PoE.

Note 2 — You can view information about power consumption and availability on the PoE tab of the shelf properties form for the 7210 SAS-T ETR.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the port object on a 7210 SAS-T ETR device. The path is Network→*NE*→Shelf→Card Slot *n*→Daughter Card Slot *n*→Port *n*/*n*/*n*.

3 Right-click on port 19, 20, 21, or 22 and choose Properties. The Physical Port (Edit) form opens with the General tab displayed.

4 Click on the PoE tab.

5 Configure the PoE Mode parameter.

6 Click on the Apply button. A dialog box appears.

7 Click on the Yes button. The Physical Port (Edit) form reappears.

8 View the information about the PoE connection.

9 Close the Physical Port (Edit) form.

Procedure 16-19 To configure PoE ports on a 7705 SAR-H

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the 7705 SAR-H where you want to configure PoE and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf object and the Card Slot object.

4 Right-click on the Daughter Card Slot object and choose Properties. The Daughter Card Slot (Edit) form opens.

5 Configure the PoE Power Supply Source parameter in the PoE panel.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The Daughter Card Slot (Edit) form closes.

8 Navigate to the port object where you want to configure PoE. The path is Network→NE→Shelf→Card Slot→Daughter Card Slot→Port n/n/n.

9 Right-click on Port 5, 6, 7, or 8 and choose Properties. The Physical Port (Edit) form opens with the General tab displayed.

Note — Only ports 5, 6, 7 or 8 support PoE, and only ports 5 and 7 support PoE Plus.

10 Click on the PoE tab.

11 Configure the PoE Mode parameter.

Note 1 — If you set the PoE Power Supply Source parameter to Internal in step 5, you can only configure ports 5 and 6:

- port 5 to PoE Plus and port 6 to Disabled
- port 5 to Standard and port 6 to Standard

Note 2 — If you set the PoE Power Supply Source parameter to External in step 5, you must set the PoE power supply source on all ports to Disabled in the PoE Mode parameter on the Physical Port (Edit) form before you configure the PoE Power Supply Source parameter for ports 7 and 8 to External.

Note 3 — You cannot configure PoE on port 6 when port 5 is configured as PoE Plus.

12 Click on the OK button to save the configuration changes. A dialog box appears.

13 Click on the Yes button. The Physical Port (Edit) form closes.

Procedure 16-20 To configure PoE ports on a 7705 SAR-W daughter card

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the Card Slot and the Daughter Card Slot objects. The six ports on the daughter card are displayed.

3 Right-click on either Port 4 or 5 and choose Properties from the contextual menu. The Physical Port (Edit) form opens with the General tab displayed.

4 Click on the PoE tab.

5 Configure the parameters:

- Slot Id
- Power Class
- PoE mode
- PoE Status
- Port Id
- Power State

6 Set the PoE Mode to PoE Plus to enable PoE.

7 Click on the OK button to save the configuration changes and close the form.

Procedure 16-21 To configure a 7705 SAR ASAP channelized TDM port

This procedure applies to 7705 SAR channelized TDM DS1/E1 ports and channelized TDM DS3/E3 ports.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the port object where you want to configure a 7705 SAR ASAP channelized TDM port. The path is Network→*NE*→Shelf→Card Slot *n*→Daughter Card Slot *n*→Port *n*/*n*/*n*.

3 Right-click on a port object that contains a channelized port (DS1/E1 or DS3/E3) and choose Properties. The Physical Port (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- Description
- Current OLC State

5 Click on the DS1/E1 or DS3/E3 tab.

6 Configure the parameters:

- Port Type
- Line Length
- Line Impedance

All ports of the ASAP daughter card are automatically configured to the same port type when the first port is configured. A mix of DS1 and E1 ports or DS3 and E3 ports is not supported. The Port Type parameter can only be modified when no channels are configured on any port of the daughter card. If all of the channels are deleted on the daughter card, the port type is automatically set to DS1 or DS3 for all ports.

7 Click on the States tab.

8 Configure the Administrative State parameter.

9 Click on the OK button. A dialog box appears.

10 Click on the OK button. The Physical Port (Edit) form closes.

Procedure 16-22 To configure a 7710 SR channelized TDM DS1 or E1 port

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you need to configure a 7710 SR channelized TDM DS1 or E1 port and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level and click on a 7710 SR port object that contains a channelized DS1 or E1. The Physical Port (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Description
- Current OLC State

6 Click on the DS1/E1 tab.

7 Configure the parameters:

- Port Type
- Line Buildout
- Line Length
- Db Loss

8 Click on the States tab.

9 Configure the Administrative State parameter.

10 Click on the OK button. A dialog box appears.

11 Click on the OK button. The Physical Port (Edit) form closes.

Procedure 16-23 To configure OmniSwitch Ethernet ports

Perform the steps in this procedure as required depending on the OmniSwitch chassis type and port type that you are configuring. Different chassis types display different port configuration parameters.



Note — You can configure MVRP fixed ports, 802.1 Q ports, aggregate ports, and VLAN Stacking Network ports.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the OmniSwitch NEs icon.

3 Right-click on the device for which you need to configure an OmniSwitch Ethernet port and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 On the Network Element (Edit) form navigation tree, expand the Shelf icon to the port level and click on a port object. The Physical Port (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Description
- Mode

  An access port is used for customer-facing traffic on which VLAN services are configured.

  A network port or channel is configured for network access in the service provider transport or infrastructure network. Typically, only one OmniSwitch network port is required for tree topology, and two ports are required for ring topology.
- Speed
- MTU (bytes)
- Automatic VLAN Binding
- Current OLC State

The Automatic VLAN Binding parameter is only supported on Stacked VLANs.

6 Click on the States tab.

7 Configure the Administrative State parameter.

8 Click on the Policies tab.



Note — A port must have a service access point associated with it before you can apply a UNI policy to the port.

9 Click on the Select button in the UNI Profile panel to assign a UNI policy to the port. The Select UNI Profile - Physical Port form opens.

10 Choose a User Network Interface (UNI) profile policy from the list and click on the OK button. The Select UNI Policy - Physical Port form closes.

11 Click on the Ethernet tab. The Ethernet port configuration form opens with the General tab displayed.

12 Perform one of the following:

a For OS 6900 and OS 10K devices, configure the following parameters:

- Duplex
- Enable Broadcast Limit Mode
- Broadcast Limit
- Enable Multicast Limit Mode
- Multicast Limit
- Enable Unknown Unicast Limit Mode
- Unknown Unicast Limit
- Type

b For all other OmniSwitch devices, configure the following parameters:

- Duplex
- Auto-negotiate
- Enable Port Mobility
- Dot1 Q Acceptable Frames
- Broadcast Limit (kbps)
- Enable Multicast Limit Mode
- Inter-Frame Gap (bytes)
- Detection
- Default VLAN Restore
- Default VLAN Enable
- Ignore BPDU
- Authenticate
- Ingress Filtering

The Inter-Frame Gap (bytes) parameter is only configurable on Gigabit Ethernet ports.

The Default VLAN Restore, Default VLAN Enable, Ignore BPDU, Authenticate, and Ingress Filtering parameters are only configurable when the Enable Port Mobility parameter is set to Enable.

13 Click on the LLDP tab, if required. The LLDP configuration form opens with the Nearest Bridge tab displayed.

14 Configure the parameters:

- Administrative Status
- Notifications
- Transmit Management Address
- LLDP TLVs

15 Click on the Remote Peers sub-tab under the LLDP tab to search for and display LLDP remote peers that are associated with the port. The remote peers are used to determine the physical topology of the network.

16 Click on the MVRP tab to configure MVRP, if required.

17 Configure the parameters on the General tab:

- Status
- Registration Mode
- Applicant Mode
- Periodic Transmission Status
- Join Timer
- Leave Timer
- Leave All Timer
- Periodic Timer

18 Click on the VLAN Restrictions tab to configure VLAN restrictions, if required:

i Click on the Create button. The MVRP VLAN Registration form appears.

ii Configure the parameters:

- VLAN
- Restrict-Static-VLAN-Registration
- Restrict-Registration
- Restrict-Advertisement

iii Click on OK to close the MVRP VLAN Registration form. The list on the VLAN Restrictions tab is updated with the new MVRP VLAN Registration entry.

19 Click on the QoS tab, if required. The QoS configuration form opens with the General tab displayed.

20 Configure the parameters:

- Trusted
- Default 802.1p
- Default DSCP
- Max Egress BW (kbps)
- Max Ingress BW (kbps)
- Servicing Mode
- Default Classification



Note — The Servicing Mode parameter does not apply to OS 6900 and OS 10K devices.

21 Perform on the following:

a For OS 6900 and OS 10K devices, go to step 26.

b For all other OmniSwitch devices, go to step 22.

22 Click on the Queue tab.

23 If you specified WRR or DRR for the Servicing Mode parameter, configure the Q0 to Q7 parameters in the Weight panel.

24 Configure the Q0 to Q7 parameters in the Minimum Bandwidth (Kbps) panel.

25 Configure the Q0 to Q7 parameters in the Maximum Bandwidth (Kbps) panel.

26 Click on the DHCP Snooping tab, if required. The tab is only available when the port is associated with a VLAN that has DHCP snooping enabled or DHCP snooping is enabled at the switch level.

27 Configure the parameters:

- Trust Mode
- IP Source Filtering

28 Click on the Ethernet Hybrid tab, if required. The tab is only available for hybrid Ethernet ports.

29 Configure the parameters:

- Mode
- Speed
- Duplex
- Auto-negotiate
- Detection

30 Click on the PoE tab, if required. The tab is only available for PoE ports.

31 Configure the parameters:

- Power State
- Maximum Power (milliwatt)
- Power Priority

32 Click on the LPS Learned MAC Entries tab to view the MAC addresses learned on the port. LPS must be enabled on the port. See Procedure 23-63 for information about configuring LPS on an Ethernet port.

33 Click on the Create button to add static MAC address entries, if required. The MAC Entries (Create) form opens.



Note — A port must be LPS-enabled and belong to a VLAN before you can add static MAC addresses to the port.

34 Click on the Select button. The Select VLAN Site - MAC Entries form opens.

35 Configure the filter criteria. A list of VLANs appears at the bottom of the Select VLAN Site - MAC Entries form.

36 Choose a VLAN from the list.

37 Click on the OK button. The Select VLAN Site - MAC Entries form closes.

38 Configure the MAC Address parameter and click on the Apply button to save the changes

39 Repeat steps 33 to 38 to add another MAC address, if required.

40 Click on the OK button. A dialog box appears.

41 Click on the Yes button. The Select VLAN Site - MAC Entries form closes.

42 Click on the OK button. The Physical Port (Edit) form closes.

Procedure 16-24 To configure OmniSwitch PoE Ports

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on an OmniSwitch object and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf object.

4 Click on a slot object. The Card Slot (Edit) form opens with the General tab displayed.

5 Click on the PoE tab.

6 Configure the parameters:

- Slot Priority
- Power State
- Port Maximum Power (MilliWatts)
- Maximum Power (Watts)
- Enable Priority Disconnect
- Enable Power Capacitor Detection
- Combo Port

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The Card Slot (Edit) form closes.

16.7 Channel and framing link configuration procedures

Use the following procedures to manage channels and framing links using the navigation tree.

Procedure 16-25 To configure SONET clear channels

Perform this procedure to configure SONET clear channels on OC3 to OC192 ports that provide clear channel services. Each port supports one clear channel.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to create a clear channel port and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level and click on a clear channel port object. The Physical Port (Edit) form opens with the General tab displayed. SONET is the default framing scheme.



Note — A clear channel port is a port on a card that is not designated Deep Channelized.

5 Configure the parameters:

- Description
- Speed

6 Click on the Apply button.

7 In the navigation tree, right-click on the port and choose Create Channel. The Channel (Create) form opens with the General tab displayed. If there are no channels available on that port, the Create Channel menu option menu is dimmed.

8 Configure the parameters:

- Description
- Configured MAC
- Mode
- Encapsulation Type
- MTU (bytes)
- DDM Event Suppression
- Load Balance Algorithm

The Encapsulation Type parameter is configurable when the Mode parameter is set to Access.

The DDM Event Suppression parameter is configurable only on ports on SFPs and XFPs optical modular transceivers.

9 Click on the Apply button to save the changes. The STS*n* clear channel appears in the navigation tree under the port of the daughter card.

a If the Encapsulation Type parameter of the port is ATM, the form is refreshed.

b If the Encapsulation Type parameter of the port is not ATM, go to step 14.

10 Click on the Edit ATM button. If the Edit ATM button is not visible, click on the More Actions button and choose Edit ATM to configure the ATM interface. The ATM interface form opens with the General tab displayed.

11 Configure the parameters:

- ATM Interface Cell Format
- ATM Minimum VPI Value
- Interface Mapping

12 To create an ILMI link, see Procedure 16-38.

13 Click on the OK button. The ATM Interface form closes.

14 Close the Channel (Edit) form.

Procedure 16-26 To perform a bulk channel creation on ports that support multiple sub-channels

Perform this procedure to create the maximum number of channels on ports that support multiple sub-channels. Table 16-5 lists the port types that support bulk channel creation.

Table 16-5 Bulk channel creation support

Node	OC3	OC12	DS3 ASAP	E3 ASAP	APS common port	APS SONET VTG
7450 ESS	X	X	X	X	X	X
7705 SAR-M	X	—	—	—	X	X
7710 SR	X	X	X	X	X	X
7750 MG	X	X	X	X	X	X

Note — This procedure assumes you have pre-configured a NE with an appropriate daughter card that supports multiple sub-channels.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Locate and expand the device on which you need to perform a bulk channel creation.

3 Perform one of the following:

a For OC3, OC12, DS3 ASAP, and E3 ASAP ports, right-click on a port icon and choose Create Maximum # of Channels from the contextual menu. The Create Maximum # of Channels form opens.

b For APS common ports and APS SONET VTGs, right click on an APS Common Config SONET channel icon and choose Create Maximum # of Channels from the contextual menu. The Create Maximum # of Channels form opens.

Note — APS common ports and APS SONET VTGs are created when you create APS groups. See Procedure 34-1 for more information.

4 Configure the parameters, as required:

- Channel Type
- STs1 Channel Payload Type
- Ds3 Channel Payload Type
- Vt15 Channel Payload Type
- Time Slots per DS0 Channel Group
- Encapsulation Type

5 Click on the Execute button. The channels and sub-channels appear in the navigation tree under the port of the daughter card.

Procedure 16-27 To configure SONET sub-channels

SONET sub-channels are available on deep channelized OC12 and OC3 ports. SONET STS1 channels support the following payload types:

- DS3
- VT15
- VT2

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure SONET sub-channels and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level, right-click on a port object and choose Create Channel. The Create Channel form opens with the General tab displayed.



Note — When there are no channels available on that port, the Create Channel menu option menu is dimmed

5 Configure the parameters:

- Local Channel ID
  - For an OC3 port, use a value from 1 to 3.
  - For an OC12 port, use a value in the format <1 to 4>.<1 to 3>
- Payload Type
- DDM Event Suppression

The DDM Event Suppression parameter is configurable only on ports on SFPs and XFPs optical modular transceivers.

6 Click on the Apply button.

The STS1 (AU3) channel appears in the navigation tree under the port of the daughter card.

7 Create the STS1 (AU3) sub-channels according to the payload type configured:

a To create VT15 (Sdh TU11) sub-channels, go to Procedure 16-29.

b To create VT2 (Sdh TU12) sub-channels, go to Procedure 16-29.

c To create a DS3 or E3 (SDH framing only) clear channel, go to step 8.

8 To create a DS3 or E3 clear channel, perform the following steps:

i From the navigation tree, select an STS1 or AU3 channel and choose Create Channel from the contextual menu. The DS3/E3 Channel (Create) form opens.

- For AU3 channels, DS3 and E3 channelization is available.
- For STS1 channels, only DS3 channelization is available.

ii Configure the Description parameter.

iii Configure the Channelized parameter.

- Choose Ds1 to channelize the DS3 to carry up to 28 DS1 channelized to the DS0 level.
- Choose E1 to channelize the DS3 to carry up to 21 E1 channelized to the DS0 level.
- Choose None to create a DS3 or E3 clear channel. Configure the following parameters:
  - Configured MAC
  - Encapsulation Type
  - Speed
  - MTU (bytes)
  - Load Balance Algorithm

iv Click on the OK button.

If you set the Channelized parameter to None, a DS3 clear channel in Access mode is created under the STS1 or the AU3 in the navigation tree.

If you set the Channelized parameter to DS1, a DS3 channelized for DS1 is created under the STS1 (AU3). Go to step 11 in Procedure 16-33 to create the DS1 channels.

If you set the Channelized parameter to E1, a DS3 channelized for E1 is created under the STS1 (AU3) in the navigation tree. Go to step 11 in Procedure 16-33 to create the E1 channels.

Procedure 16-28 To configure SDH sub-channels

SDH sub-channels are available on deep channelized OC12 and OC3 ports. SDH AU4 channels support the following payload types:

- TU3
- TU11
- TU12

SDH AU3 channels support the following payload types:

- DS3
- E3
- TU11
- TU12

Perform this procedure to configure SDH sub-channels on ports that provide channelized services. You must first configure port framing to SDH since default framing on SONET/SDH ports is SONET.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure SDH sub-channels and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level and click on a deep channelized port. The Physical Port (Edit) form opens with the General tab displayed.

5 Click on the SONET tab and set the Framing parameter to SDH.

6 Click on the OK button.

7 Right-click on the port again and choose Create Channel from the contextual menu. The Channel Type Selection form opens.

8 Choose one of the following channel types and click on the OK button:

a SONET Sts1 (Sdh Au3).

SONET STS1 channelization and SDH AU3 channelization are equivalent. Go to step 5 of Procedure 16-27.

b SONET Sts3 (Sdh Stm1).

The Sts3 SONET Channel (Create) form opens with the General tab displayed. If there are no channels available on that port, the Create Channel menu option menu is dimmed.

The Payload Type parameter for SDH STM1 (AU4) is set to TUG3. There is no SONET framing equivalent. Go to step 9.

9 Configure the parameters:

- Description
- Local Channel ID

10 Click on the States tab.

11 Configure the Administrative State

12 Click on the OK button. The STM1 (AU4) channel appears in the navigation tree under the port of the daughter card. It contains three TUG3 groups.

13 Right-click on a TUG3 group and choose Properties from the contextual menu. The Sdh Tug3 (Edit) form opens with the General tab displayed.

14 Choose one of the following options to configure the Payload Type parameter:

a PDH Tu3. Click on the Cancel button and go to step 15 to create a TU3 channel.

b SONET VT15 (SDH Tu11). Click on the Apply button and go to Procedure 16-29.

c SONET VT2 (SDH Tu12). Click on the Apply button and go to Procedure 16-29.

15 To create a TU channel, right-click on the TUG3 group and choose Create Channel from the contextual menu. The TU3 Channel (Create) form opens.

16 Configure the parameters:

- Description
- Payload Type

17 Click on the States tab.

18 Configure the Administrative State.

19 Click on the OK button. A TU3 channel is created under the TUG3 group in the navigation tree.

20 Right-click on the Tu3 and choose Create Channel from the contextual menu. The DS3/E3 Channel (Create) form opens with the General tab displayed.

The E3 is the only payload type available.

21 Configure the parameters:

- Description
- Configured MAC
- Encapsulation Type
- Speed
- MTU (bytes)
- Load Balance Algorithm

22 Click on the States tab.

23 Configure the Administrative State

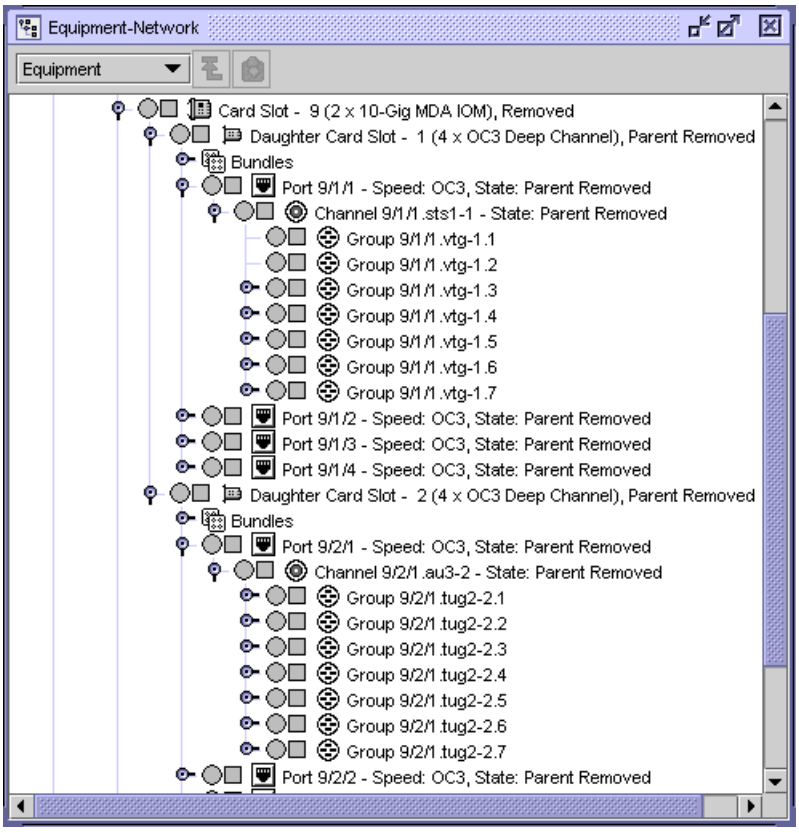
24 Click on the OK button. An E3 clear channel is created under the AU4/TUG3 in the navigation tree.

Procedure 16-29 To create VT15 (TU11) or VT2 (TU12) sub-channels

A SONET VTG and an SDH TUG2 are equivalent groups. A VTG contains four VT15 channels or three VT2. A TUG2 contains four TU11 channels or three TU12. An SDH TUG 3 has no SONET equivalent, however, it contains seven TUG2. (An STM1/AU4 contains three TUG3). See "Comparison of SONET and SDH hierarchies" in section 16.3.

An STS1 channelized to carry a VT15 or VT2 payload type contains seven VTG. An AU3 or a TUG3 channelized to carry a TU11 or TU12 payload type contain seven TUG2. STS1 and AU3 channelization are shown in Figure 16-11.

Figure 16-11 SONET VTG and SDH TUG2 in navigation tree



Each VTG (TUG2) supports up to four VT15 (TU11) channels or three VT2 (TU12) channels. Create each VTG/TUG2 channel one at time.

1 Complete Procedure 16-27 or Procedure 16-28 to carry a VT15 (TU11) or VT2 (TU12) payload type.

   a Go to step 2 to create a VT15 (TU11) channel.

   b Go to step 3 to create a VT2 (TU12) channel.

2 To create a VT15 (TU11) channel, perform the following steps:

   i Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

   ii Right-click on the device where you want to create a VT15 (TU11) channel and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

   iii On the Network Element (Edit) form navigation tree, expand the Shelf icon.

   iv Expand to the channel level, right-click on a VTG or TUG2 channel group that is to carry a VT15 (TU11) payload and choose Create Channel from the contextual menu. The SONET VT (SDH Tu) Channel (Create) form opens.

   v Configure the parameters:

   - Local Channel ID
     Set the Local Channel ID to a value in the range 1 to 4 since there are four VT15 (TU11) in a VTG (TU2).
   - Description

   The default payload type for a VT15 (TU11) channel is PDH DS1. There is no other available payload type.

   vi Click on the OK button. A VT15 channel is created under the VTG or a TU11 channel is created under the TUG2 in the navigation tree.

   vii Right-click on a VT15 or TU11 channel and choose Create Channel from the contextual menu. The DS1/E1 Channel (Create) form opens.

   The Local Channel ID is equal to the VT15 channel Local Channel ID parameter and the channel type is set to DS1 since a VT15 or TU11 channel supports one DS1.

   viii Click on the OK button A DS1 channel is created under the VT15 or the TU11 in the navigation tree.

   You can create up to 28 VT15 (TU11) channels on a VTG (TUG2).

ix Repeat steps 1 and 2 for each VT15 (TU11) channel that you want to create.

x Since a DS1 channel is not used as a SAP, create a DS0 group for each DS1 channel created. Go to step 12 of Procedure 16-33.

3 To create a VT2/TU12 channel, complete these steps:

i From the navigation tree, select a VTG or TUG2 channel group to carry a VT2 (TU12) payload and choose Create Channel from the contextual menu. The SONET VT (SDH Tu) Channel (Create) form opens.

ii Configure the parameters:

- Local Channel ID

  Set the Local Channel ID to a value in the range 1 to 3 since there are three VT2 (TU12) in a VTG (TUG2).
- Description
- Payload Type

  PDH E1 is not available for SONET framing.

iii Click on the OK button. A VT2 channel is created under the VTG, or a TU12 channel is created under the TUG2 in the navigation tree.

iv Right-click on the VT2 or TU12 channel and choose Create Channel from the contextual menu. The DS1/E1 Channel (Create) form opens.

The Local Channel ID is equal to the VT2 channel Local Channel ID parameter, since a VT2 channel supports one E1 or DS1.

v Click on the States tab.

vi Configure the Administrative State parameter.

vii Click on the OK button. A DS1 channel is created under the VT2 in the navigation tree. An E1 or DS1 is created under the TU12. You can create up to 21 VT2 (TU12) channels on a VTG (TUG2).

viii Repeat steps 1 and 2 for each VT2 (TU12) that you want to create.

ix Since a DS1/E1 channel is not used as a SAP, create a DS0 group for each DS1 or E1 channel created. Go to step 12 of Procedure 16-33.

Procedure 16-30 To create TDM DS1 or E1 channels

Perform this procedure to create DS1/E1 channels and child objects on a channelized DS1/E1 port.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure TDM DS1 or E1 channels and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level and click on a port. The Physical Port (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Description
- Current OLC State
- Revert OLC State

6 Select the DS1/E1 tab and configure the parameters:

- Port Type
- Line Length

7 Click on the OK button.

8 Right-click on the port again and choose Create Channel from the contextual menu. The DS1/E1 Channel (Create) form opens. If there are no channels available on that port, the Create Channel menu option is dimmed.

9 Click on the OK button.

10 To create DS0 channel groups, complete these steps:

i From the navigation tree, right-click a DS1 or E1 channel under the required port and choose Create Channel from the contextual menu. The DS0 Channel Group (Create) form opens with the General tab displayed.

ii Configure the parameters:

- Local Channel ID
  For a DS0 group from a DS1 choose from 1 to 24. For a DS0 group from an E1, choose from 2 to 32.
- Description
- Mode
- Encapsulation Type
- MTU (bytes)



Note 1 — All channel groups on a 7705 SAR ASAP port must have the same mode configured. When the first channel group is configured, all other channel groups on the port must be set to the same mode.

Note 2 — The default encapsulation type for the 7705 SAR is N/A. The encapsulation type must be changed from N/A to a valid type. For instance, to support CAS signaling, the encapsulation type must be set to CEM. After a valid encapsulation type is configured for a channel group, the encapsulation type cannot be changed for that channel group. To change the encapsulation type, the channel group must be deleted and recreated.

Note 3 — On a 16/32x Channelized ASAP, you must configure the MDA mode in order to use certain encapsulation types. See Procedure 15-33 for more information on configuring the MDA mode.

iii Click on the Channel Group tab.

iv Configure the parameters:

- Time Slots
  Choose one or more timeslots. You can use the Select All and Deselect All buttons.
- Idle Payload Fill Type
- Idle Payload Fill Pattern
- Idle Signal Fill Type
- Idle Signal Fill Pattern
- BER SF Link Down
- Signal Mode

v Click on the OK button. The timeslot is assigned to the DS0 channel group in the navigation tree.

Procedure 16-31 To configure TDM DS1 or E1 channels

Perform this procedure to configure DS1/E1 channel parameters and child objects on a channelized DS1/E1 port, add a DS0 channel group, collect and view performance statistics, or view alarm information.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device you need to configure TDM DS1 or E1 channels and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Expand the Shelf icon to the channel level and choose a DS1 or E1 channel. The DS1/E1 Channel (Edit) form opens with the General tab displayed.

4 Click on the States tab.

5 Configure the Administrative State parameter.

6 Click on the Channel tab button. The DS1/E1 Channel (Edit) form opens.

7 Configure the parameters, if applicable:

- Channel Framing
- Clock Source
- Loopback
- Report Alarms
- Hold Time Up (100s of milliseconds)
- Hold Time Down (100s of milliseconds)
- Respond to Remote Loop Signal
- Signal Mode
- Threshold for BER SD Notifications
- Threshold for BER SF Notifications
- Synchronous Status Messages
- E1 Tx DUS/DNU
- E1 SSM-Bit



Note 1 — The Synchronous Status Messages, E1 Tx DUS/DNU, and E1 SSM-Bit parameters are configurable only on E1 channels in a Release 6.0 or later 7705 SAR.

Note 2 — The Clock Source parameter value Differential is only supported on a 16/32 × Channelized DS1/E1 ASAP v2 in a Release 6.0 R1 or later 7705 SAR-8, 7705 SAR-8 v2, or 7705 SAR-18, a 4 × Channelized DS3/E3 ASAP in a Release 6.0 R3 or later 7705 SAR, and an ASAP channelized card in a Release 6.0 R2 or later 7705 SAR-A.

Note 3 — If you create an MLPPP bundle and the DS1 BER exceeds a threshold, the PPP link is automatically removed from the MLPPP bundle.

8 Add a DS0 channel group, if required.

i Click on the SubChannels tab.

ii Click on the Create Cha... tab. The DS0 Channel Group (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Local Channel ID
- Description
- Mode
- Encapsulation Type
- MTU (bytes)



Note 1 — On a 16/32x Channelized ASAP, you must configure the MDA mode in order to specify the encapsulation type. See Procedure 15-33 for more information about configuring the MDA mode.

Note 2 — You must set the value of the Encapsulation Type parameter to CEM if you are configuring an MDA card of type 16 × Channelized DS1/E1 ASAP v2 or 32 × Channelized DS1/E1 ASAP v2 on a 7705 SAR-8 or 7705 SAR-18.

iv Click on the OK button. The DS0 Channel Group (Create) form closes and a dialog box appears.

v Click on the OK button.

9 Click on the Statistics tab to collect and view performance statistics, if required.

10 Perform one of the following:

- **a** Click on the Collect button to collect performance statistics data on demand. The collected statistics are listed on the form.
- **b** Click on the Collect All button to collect one on-demand statistics record for each statistic type that the object supports. The collected statistics are listed on the form.

11 Choose a statistic from the list and click on the Properties button. The Statistics Record form opens.

12 View the statistics data, if required.

13 Close the Statistics Records form.

14 Click on the Faults tab to view alarm information, if required.



Note — If are configuring a 7705 SAR and selected a clock source of adaptive, you can click on the Adaptive Clock History tab to view channel adaptive clock performance data for the preceding 15 min.

15 Click on the OK button. A dialog box appears.

16 Click on the Yes button. The DS1/E1 Channel (Edit) form closes.

Procedure 16-32 To create serial channels

Perform this procedure to create serial channel and child objects from a Serial Data Interface port.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the device where you want to configure serial channels and expand to the port level.

3 Right-click on the port and choose Create Channel from the contextual menu. The Serial Channel (Create) form opens. If there are no channels available on that port, the Create Channel menu option is dimmed.

4 Click on the States tab.

5 Configure the Administrative State parameter.

6 Click on the Apply button. The Serial Channel (Edit) form refreshes with additional tabs.

7 Click on the Channel tab.

8 Configure the parameters:

- Device Mode
- Gender
- Speed
- Loopback
- Multidrop Data Bridge
- S-Bit Signalling
- HCM Data Position
- Character Length
- Parity
- Stop Bits
- Report Alarms
- DTR / DSR Input
- RTS / DCD / C / I Input
- ALB / CTS Input
- RDL / RI Input
- DSR / DTR Output
- DCD / RTS / I / C Output
- CTS / ALB Output
- RI / RDL Output
- Hold Time Up (milliseconds)
- Hold Time Down (milliseconds)

Depending on the serial type of the configured port, different parameters are configurable in the Control Leads panel.

9 Create DS0 channel groups:

i Click on the SubChannels tab.

ii Click on the Create Cha... button. The DS0 Channel Group (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Description
- Encapsulation Type
- MTU (bytes)



Note 1 — The default encapsulation type for the 7705 SAR is N/A. The encapsulation type must be changed from N/A to a valid type. After a valid encapsulation type is configured for a channel group, the encapsulation type cannot be changed for the channel group. To change the encapsulation type, the channel group must be deleted and re-created.

Note 2 — On an SDI MDA, you must configure the serial type to X.21 or V.35 to use the FR, HDLC, or cHDLC encapsulation types. See Procedure 16-12 for more information.

iv Click on the OK button. The DS0 Channel Group (Create) form closes.

10 Close the Serial Channel (Edit) form.

Procedure 16-33 To create TDM DS3 channels

Perform this procedure to create DS3 channel and children objects from a channelized DS3 port.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to create a TDM DS3 channel and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level and click on a port. The Physical Port (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Description
- Current OLC State

6 Choose the DS3/E3 tab and configure the parameters:

- Line Buildout
- Type. Choose DS3.

7 Click on the OK button.

8 Right-click on the port again and choose Create Channel from the contextual menu. The DS3/E3 Channel (Create) form opens. If there are no channels available on that port, the Create Channel menu option is dimmed.

9 To create the DS3/E3 channel, complete these steps:

a Configure the Channelized parameter to DS1 or E1, if you want to channelize to the DS0 level.

b Configure the Channelized parameter to None if this is a clear channel application.

Configure the parameters, if applicable:

- Description
- Mode
- Configured MAC
- Encap Type
- Speed
- MTU (bytes)
- Load Balance Algorithm

The Local Channel ID parameter is configured automatically and the Mode parameter is always Access for TDM.

Note 1 — On a 4x Channelized ASAP, you must configure the MDA mode in order to use certain encapsulation types. See Procedure 15-33 for more information on configuring the MDA mode.

Note 2 — If you want to configure a DS3/E3 channel as a network interface on a channelized ASAP MDA, see Procedure 16-35.

10 Click on the OK button.

If this is a Channelized DS1 or E1 application, continue to step 11.

11 To create DS1 or E1 channels, complete these steps:

i From the navigation tree, select a DS3 channel and choose Create Channel from the contextual menu. The Create DS1/E1 Channel form opens.

ii Configure the Local Channel ID parameter.

- For DS1 choose from 1 to 28.
- For E1 choose from 1 to 21.

iii Click on the OK button. The DS1 or E1 channels are created under the DS3 in the navigation tree.

12 To create DS0 channel groups, complete these steps:

i From the navigation tree, select a DS1 or E1 channel and choose Create Channel from the contextual menu to create DS0 groups. The DS0 Channel (Create) form opens with the General tab displayed.

ii Configure the parameters:

- Local Channel ID
- Description
- Configured MAC
- Mode
- Encap Type
- Speed
- MTU (bytes)
- Load Balance Algorithm

For a DS0 group from a DS1 choose from 1 to 24 for the Local Channel ID parameter. For a DS0 group from an E1, choose from 2 to 32.

Note — On a 4x Channelized ASAP, you must configure the MDA mode in order to use certain encapsulation types. See Procedure 15-33 for more information on configuring the MDA mode.

iii Click on the Channel Group tab.

iv Configure the parameters:

- CRC Precision
- Idle Cycle Flags
- Time Slots
- BER SF Link Down

v Click on the OK button. The timeslot is assigned to the DS0 channel group in the navigation tree.

Procedure 16-34 To configure TDM DS3 channels

Perform this procedure to configure DS3 channels and children objects from a channelized DS3 port.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure TDM DS3 channels and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the channel level and click on a DS3 channel. The DS3/E3 Channel (Edit) form opens with the General tab displayed.

5 Configure the Description parameter.

6 Configure the Channelized parameter and click on the Apply button.

a If you choose None, go to step 7.

b If you choose DS1 or E1, perform steps 12 to 35.

7 Configure the parameters:

- Configured MAC
- Speed
- MTU (bytes)
- Load Balance Algorithm

8 Configure the Encapsulation Type parameter and click on the Apply button.

a If you choose BCP Null, BCP DOT1 Q, or IPCP, go to step 9.

b If you choose FR, go to step 10.

c If you choose Cisco HDLC, go to step 11.

d If you choose WAN Mirror, perform steps 13 to 22.

9 Configure the PPP interface for the channel, if required. Perform the following steps:

i Click on the Edit PPP button. If the Edit PPP button is not visible, click on the More Actions button and choose Edit PPP. The PPP Interface form opens with the General tab displayed.

ii Configure the parameters:

- Period
- Drop Count

iii To view port, PPP control protocol, statistics, or alarm information for the PPP interface, click on the appropriate tab.

iv Click on the OK button. The PPP Interface form closes.

v Perform steps 13 to 22.

10 Configure the FR interface, if required. Perform the following steps:

i Click on the Edit FR button. If the Edit FR button is not visible, click on the More Actions button and choose Edit FR. The FR Interface form opens with the General tab displayed.

ii Configure the parameters:

- LMI Type
- LMI Mode
- Link Identifier
- Error Threshold
- Monitored Events
- Polling Interval (seconds)
- Full Enquiry Interval

iii Click on the Frf12 tab.

iv Set the Mode parameter to Enabled.

v Configure the Fragment Threshold parameter.

vi Click on the Select button beside the MCFR Egress QoS Profile parameter. The Select MCFR Egress Qos Profile - FR Configuration form opens.

vii Choose a profile from the list and click on the OK button. The Select MCFR Egress Qos Profile - FR Configuration form closes and the FR Interface form is refreshed with the MCFR Egress QoS Profile information.

viii To view port, statistical, or alarm information for the FR interface, click on the appropriate tab.

ix Click on the OK button. The FR Interface form closes.

x Perform steps 13 to 22.

11 Configure the Cisco HDLC information.

i Click on the Cisco HDLC tab.

ii Configure the parameters:

- Keep Alive (seconds)
- Up Count
- Down Count

iii Perform steps 13 to 22.

12 Configure the DS1 and DS0 channels. Perform the following steps:

i Click on the SubChannels tab.

ii Click on the Create button. The DS1/E1 Channel (Create) form opens with the General tab displayed.

iii Configure the Local Channel ID parameter.

iv Click on the States tab.

v Configure the Administrative State parameter.

vi Click on the OK button. The DS1/E1 Channel (Create) form closes.

13 Click on the States tab.

14 Configure the Administrative State parameter.

15 Click on the Channel tab. The DS3/E3 Channel (Edit) form opens.

16 Configure the parameters, if applicable:

- Channel Framing
- CRC Precision
- Clock Source
- Idle Cycle Flags
- Loopback
- Subrate CSU Mode
- Subrate Range
- Loop Respond
- Report Alarms
- Bit Error Insertion Rate (E3 only)
- Pattern (E3 only)
- Duration (seconds) E3 only

Note — The Clock Source parameter value Differential is only supported on a 16/32 × Channelized DS1/E1 ASAP v2 in a Release 6.0 R1 or later 7705 SAR-8, 7705 SAR-8 v2, or 7705 SAR-18, a 4 × Channelized DS3/E3 ASAP in a Release 6.0 R3 or later 7705 SAR, and an ASAP channelized card in a Release 6.0 R2 or later 7705 SAR-A.

17 Click on the Message Data Link tab.

18 Configure the parameters:

The MDL Message Type parameter specifies the Line Message Data Link message for a DS3 and specifies the transmission method of a message over a channelized interface. The parameter is only applicable if the DS3 is using C-bit framing. The default is disabled. Click on the check boxes to enable transmission methods and enter text strings to choose the message options for this parameter as required. The transmission options are:

- Test Signal
- DS3 Path
- Idle Signal

Table 16-6 describes the MDL message options.

Table 16-6 MDL message options

Option	String Length	Description
Port Number String	0 to 38 characters	specifies the port ID code
Generator Number String	0 to 38 characters	specifies the generator number to send in the MDL test signal message
Equipment ID Code	0 to 10 characters	specifies the Equipment ID code
Location ID Code	0 to 11 characters	specifies the Location ID code
Frame ID Code	0 to 10 characters	specifies the Frame ID code
Unit ID Code	0 to 6 characters	specifies the unit ID code
Facility ID Code	0 to 38 characters	specifies the facility ID code

19 Click on the Terminations tab to view channel termination information.

20 Click on the Statistics tab to view statistical information.

21 Click on the Faults tab to view alarm information.

22 Click on the OK button. The DS3/E3 Channel (Edit) form closes.

23 Right-click on a DS1 channel in the navigation tree and choose Properties from the contextual menu. The property form for the channel opens with the General tab displayed.

24 Click on the States tab.

25 Configure the Administrative State parameter, if required.

26 Add a DS0 channel group, if required. Perform the following steps:

i Click on the SubChannels tab.

ii Click on the Create button. The DS0 Channel Group (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Local Channel ID
- Description
- Configured MAC
- Encapsulation Type
- Speed
- MTU (bytes)
- Load Balance Algorithm



Note — On a 4x Channelized ASAP, you must configure the MDA mode in order to use certain encapsulation types. See Procedure 15-33 for more information on configuring the MDA mode.

iv Click on the OK button. The DS0 Channel Group (Create) form closes.

27 Click on the Channel tab.

28 Configure the parameters:

- Channel Framing
- Clock Source
- Idle Cycle Flags
- Loopback
- Bit Error Insertion Rate (E3 only)
- Pattern (E3 only)
- Duration (seconds) E3 only

29 Click on the Statistics tab to view statistical information.

30 Click on the Faults tab to view information about alarms.

31 Click on the OK button. The channel properties form closes.

32 Configure timeslots for the DS0 channel group. Perform the following steps.

i Choose a DS0 channel in the navigation tree and choose Properties from the contextual menu. The property form for the channel opens with the General tab displayed.

ii Configure the parameters, as required.

iii Click on the States tab.

iv Configure the Administrative State parameter.

v Click on the Channel Group tab.

vi Configure the parameters:

- CRC Precision
- Idle Cycle Flags
- Time Slots

  Choose one or more timeslots. You can use the Select All and Deselect All buttons.

vii If you set the Encapsulation Type parameter to BCP Null, BCP DOT1 Q, or IPCP in step ii, you can configure the PPP for the timeslot on the Channel Groups tab.

- Click on the Edit PPP button. If the Edit PPP button is not visible, click on the More Actions button and choose Edit PPP. The PPP Interface form opens with the General tab displayed.
- Configure the parameters:
  - Period
  - Drop Count
  - Compression

    The Compression parameter is configurable when the DS1 or E1 channel group is on an ASAP MDA in a 7710 SR or 7750 SR.
- Click on the OK button. The PPP Interface form closes and the DS0 Channel Group (Edit) form reappears.

33 Click on the Statistics tab to view statistical information.

34 Click on the Faults tab to view information about alarms.

35 Click on the OK button. The DS3/E3 Channel (Edit) form closes.

Procedure 16-35 To configure a DS3/E3 channel as a network interface on a channelized ASAP MDA

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure a DS3/E3 channel and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level.

5 Perform one of the following.

a If you are configuring an OC-*n* channelized ASAP MDA, right-click on an available port and choose Create Channel from the contextual menu. The Sts SONET Channel (Create) form opens with the General tab displayed; go to step 6.

b If you are configuring a DS3/E3 channelized ASAP MDA, right-click on an available port and choose Create Channel from the contextual menu. The DS3/E3 Channel (Create) form opens with the General tab displayed; go to step 11.

6 Configure the parameters:

- Local Channel ID
- Description
- Payload Type

7 Click on the States tab.

8 Configure the Administrative State parameter.

9 Click on the OK button.The Sts SONET Channel (Create) form closes and the STS1 channel appears in the navigation tree under the port of the channelized ASAP daughter card.

10 Right-click on the STS1 channel and choose Create Channel from the contextual menu. The DS3/E3 Channel (Create) form opens with the General tab displayed.

11 Configure the parameters:

- Description
- Configured MAC
- Mode
  You must set the Mode parameter to Network.
- Encapsulation Type
  The only available encapsulation type available in network mode is PPP.
- Speed
  The only available speed is line rate.
- MTU (bytes)
- Load Balance Algorithm

12 Click on the States tab.

13 Configure the Administrative State parameter.

14 Click on the Apply button. The form displays additional tabs.

15 Click on the Channel tab.

16 Configure the parameters:

- Channel Framing
- CRC Precision
- Clock Source
- Idle Cycle Flags
- Loopback
- Subrate CSU Mode
- Loop Respond
- Report Alarms

17 Click on the Message Data Link tab.

18 Configure the parameters:

The MDL Message Type parameter specifies the Line Message Data Link message for a DS3 and specifies the transmission method of a message over a channelized interface. The parameter is only applicable if the DS3 is using C-bit framing. The default is disabled. Click on the check boxes to enable transmission methods and enter text strings to choose the message options for this parameter as required. The transmission options are:

- Test Signal
- DS3 Path
- Idle Signal

Table 16-7 describes the MDL message options.

Table 16-7 MDL message options

Option	String Length	Description
Port Number String	0 to 38 characters	specifies the port ID code
Generator Number String	0 to 38 characters	specifies the generator number to send in the MDL test signal message
Equipment ID Code	0 to 10 characters	specifies the Equipment ID code
Location ID Code	0 to 11 characters	specifies the Location ID code
Frame ID Code	0 to 10 characters	specifies the Frame ID code
Unit ID Code	0 to 6 characters	specifies the unit ID code
Facility ID Code	0 to 38 characters	specifies the facility ID code

19 Click on the OK button. The DS3/E3 or Sts SONET Channel (Create) form closes and a DS3/E3 channel appears in the navigation tree under the port on the channelized ASAP MDA.

Procedure 16-36 To configure an L3 interface on a DS3/E3 channel on a channelized ASAP MDA

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure an L3 interface and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the channel level and click on a DS3/E3 channel on a channelized ASAP MDA port. The DS3/E3 Channel (Edit) form opens with the General tab displayed.

5 Click on the Policies tab to configure the policies for the DS3/E3 channel. Perform the following steps.

i Click on the Select button beside the Network Queue Policy Name parameter. The Select Network Queue Policy - DS3/E3 Channel list form opens.

ii Select a network queue policy from the list and click on the OK button. The Select Network Queue Policy - DS3/E3 Channel list form closes and the DS3/E3 Channel (Edit) form reappears.

iii Click on the Select button beside the ID parameter in the Accounting Policy panel. The Select Accounting Policy - DS3/E3 Channel list form opens.

iv Select an accounting policy from the list and click on the Ok button. The Select Accounting Policy - DS3/E3 Channel list form closes and the DS3/E3 Channel (Edit) form refreshes with the accounting policy information.

v Configure the Collect Accounting Statistics parameter.

vi Click on the Select button in the Port Scheduler Policy panel to assign a port scheduler policy to the port. The Select Port Scheduler Policy - Physical Port form opens.

vii Select a port scheduler policy from the list and click on the OK button. The Select Port Scheduler Policy - Physical Port form closes.

6 Click on the Network Interfaces tab.

7 Click on the Create button. The Create Network Interface - Routing Instance form opens.

8 Perform steps 6 to 49 of Procedure 22-9 to create a network interface on the DS3/E3 channel.

The port in step 6 of Procedure 22-9 is set to the DS3/E3 channel by default. Go to step 12 of Procedure 22-9.

9 The L3 interface appears on the Network Interfaces tab. Close the DS3/E3 Channel (Edit) form.

Procedure 16-37 To configure a PVC

PVCs are automatically created by the device when a new L3 interface over ATM is created on the 5620 SAM, and when a new ILMI link is created between ATM interfaces. See Procedure 16-38 for more information about creating ILMI links.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure a PVC and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the channel level and click on a SONET/SDH ATM clear channel. The property form for the channel opens with the General tab displayed.

5 Click on the L3 Interfaces tab.

6 Choose the appropriate interface from the list and click on the Properties button. The L3 Interface form opens.

7 Click on the ATM tab.

8 Configure the parameters:

- AAL5 Encapsulation
- ATM OAM Alarm Cell Handling

9 Click on the Apply button to save the changes.

10 To view more information about the PVC:

i Click on the View PVC Connection button. The ATM PVC Connection form opens.

ii Click on the tabs to view information for the ATM PVC connection.

11 Click on the Cancel button to close the ATM PVC Connection form, the L3 Interface form, and the channel form.

Procedure 16-38 To create an ILMI link

Perform this procedure to create an ILMI link between device ATM interfaces. This functionality is supported on the 7750 SR and 7710 SR. Ensure that ATM QoS policies are configured before you create the ILMI link. See chapter 42 for more information about creating ATM QoS policies.

1 Perform one of the following to open the ATM interface properties form.

a Use the navigation tree

i Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

ii Right-click on the device where you want to create an ILMI link and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

iii On the Network Element (Edit) form navigation tree, expand the Shelf icon.

iv Expand to the port level and click on a clear channel port. The Physical Port (Edit) form opens with the General tab displayed.



Note — A clear channel port is a port on a card that is not designated Deep Channelized.

v Click on the Channels tab.

vi Choose the appropriate channel from the list and click on the Properties button. The Channel (Edit) form opens.

vii Click on the Edit ATM button. If the Edit ATM button is not visible, click on the More Actions button and choose Edit ATM. The ATM Interface form opens with the General tab displayed.

b Use the Manage Equipment list form to search for a clear channel port with an ATM interface.

i Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

ii Choose Port from the object drop-down list.

iii Configure the filter criteria to search for ATM encapsulation types.

iv Click on the Search button. The Select form displays the results of the search.

v Select an entry by double-clicking. Alternatively, select an entry and click on the Properties button. The Select form closes and the Channel (Edit) form opens.

vi Click on the Edit ATM button. If the Edit ATM button is not visible, click on the More Actions button and choose Edit ATM. The ATM Configuration (Edit) form opens with the General tab displayed.

2 Click on the Create ILMI Link button. The Configure ILMI Link form opens with the General tab displayed.

3 Configure the parameters:

- Administrative Status
- Protocol Version
- IME Type
- Keep-Alive Polling Frequency (seconds)
- Keep-Alive Polling Count
- Keep-Alive Test Frequency (seconds)
- Restore Keep-Alive Defaults
- ILMI Link VCI
- ILMI Link VPI

The Restore Keep-Alive Defaults parameter restores the default values of the Keep-Alive Polling Frequency (seconds), Keep-Alive Polling Count, and Keep-Alive Test Frequency (seconds) parameters.

The Keep-Alive Test Frequency (seconds) parameter is configurable when the Protocol Version parameter is set to 4.0.

4 Choose an ingress ATM QoS policy by clicking on the Select button. The Select ATM Policy - ATM ILMI Link Configuration list form opens. Click on the Search button and choose an ingress ATM policy from the list to associate with the ILMI link. Click on the OK button. The Select ATM Policy - ATM ILMI Link Configuration list form closes.

5 Choose an egress ATM QoS policy by clicking on the Select button. The Select ATM Policy - ATM ILMI Link Configuration list form opens. Click on the Search button and choose an egress ATM policy from the list to associate with the ILMI link. Click on the OK button. The Select ATM Policy - ATM ILMI Link Configuration list form closes.

6 Click on the Finish button. The Configure ILMI Link form closes and the ATM Configuration (Edit) form reappears.

7 Close the ATM Configuration (Edit) form. The Channel (Edit) form reappears.

8 Close the Channel (Edit) form.

Procedure 16-39 To configure an ILMI link

1 Perform step 1 of Procedure 16-38 to open the ATM Configuration (Edit) form.

2 Click on the Edit ILMI Link button. The ILMI Link form opens with the ILMI Link Configuration tab displayed.

3 Configure the parameters, as required.

- Administrative Status
- Protocol Version
- IME Type
- Keep-Alive Polling Frequency (seconds)
- Keep-Alive Polling Count
- Keep-Alive Test Frequency (seconds)
- Restore Keep-Alive Defaults

The Restore Keep-Alive Defaults parameter restores the default values of the Keep-Alive Polling Frequency (seconds), Keep-Alive Polling Count, and Keep-Alive Test Frequency (seconds) parameters.

The Keep-Alive Test Frequency (seconds) parameter is configurable when the Protocol Version parameter is set to 4.0.

4 Choose an ingress ATM QoS policy by clicking on the Select button. The Select ATM Policy - ATM ILMI Link Configuration list form opens. Click on the Search button and choose an ingress ATM policy from the list to associate with the ILMI link. Click on the OK button. The Select ATM Policy - ATM ILMI Link Configuration list form closes.

5 Choose an egress ATM QoS policy by clicking on the Select button. The Select ATM Policy - ATM ILMI Link Configuration list form opens. Click on the Search button and choose an egress ATM policy from the list to associate with the ILMI link. Click on the OK button. The Select ATM Policy - ATM ILMI Link Configuration list form closes.

6 Click on the Peer Interface Configuration tab to view ILMI properties of the peer interface of the link.

7 Click on the OK button to close the Configure ILMI Link form. The ATM Configuration (Edit) form reappears.

8 To remove an ILMI link, click on the Remove ILMI Link button. Removing the ILMI link also removes the PVC.



Note — An ILMI link can be removed only if its Administrative Status parameter is set to Disabled.

9 Click on the Cancel button to close the ATM Configuration (Edit) form. The Channel (Edit) form reappears.

10 Click on the Cancel button to close the Channel (Edit) form.

17 — Inventory management

17.1 Inventory management overview *17-2*

17.2 Sample inventory management workflow *17-5*

17.3 Workflow to manage inventory *17-6*

17.4 Inventory management procedures *17-7*

17.1 Inventory management overview

The 5620 SAM client GUI provides multiple ways of generating inventory data about managed devices and the managed network. You can also use the 5620 SAM-O interface to generate inventory data. See “XML requests” in the *5620 SAM XML OSS Interface Developer Guide* for information about using the 5620 SAM-O interface.

Use the list, properties, and equipment management forms to generate inventories for:

- required data for SLA audits
- equipment, such as cards, needed for sparing
- installed and in-operation equipment
- vintages, CLEI codes, and identifications

You can generate inventory data based on:

- the entire managed network, which includes all 5620 SAM-managed devices
- a managed device

Note — Not all columns in the inventory lists are applicable to all equipment types. For example, not all card types have an associated CLEI code. In situations such as this, the inventory list displays “N/A” in the column.

Figure 17-1 shows how to use the Manage Equipment form to filter and inventory data for all managed devices.

Figure 17-1 Generating inventory data for all managed devices

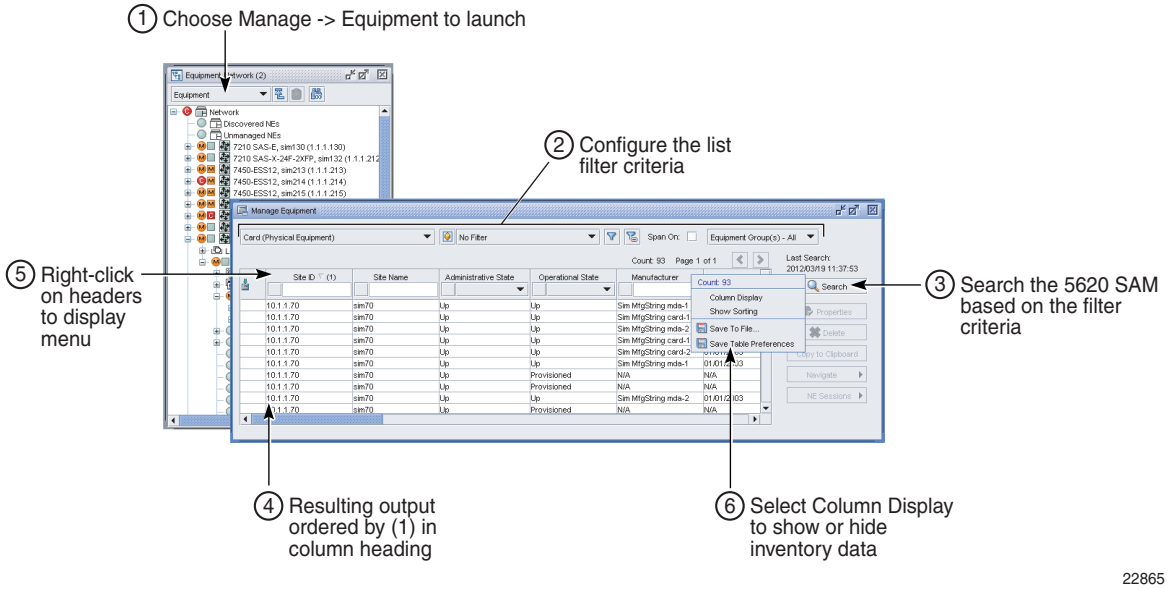
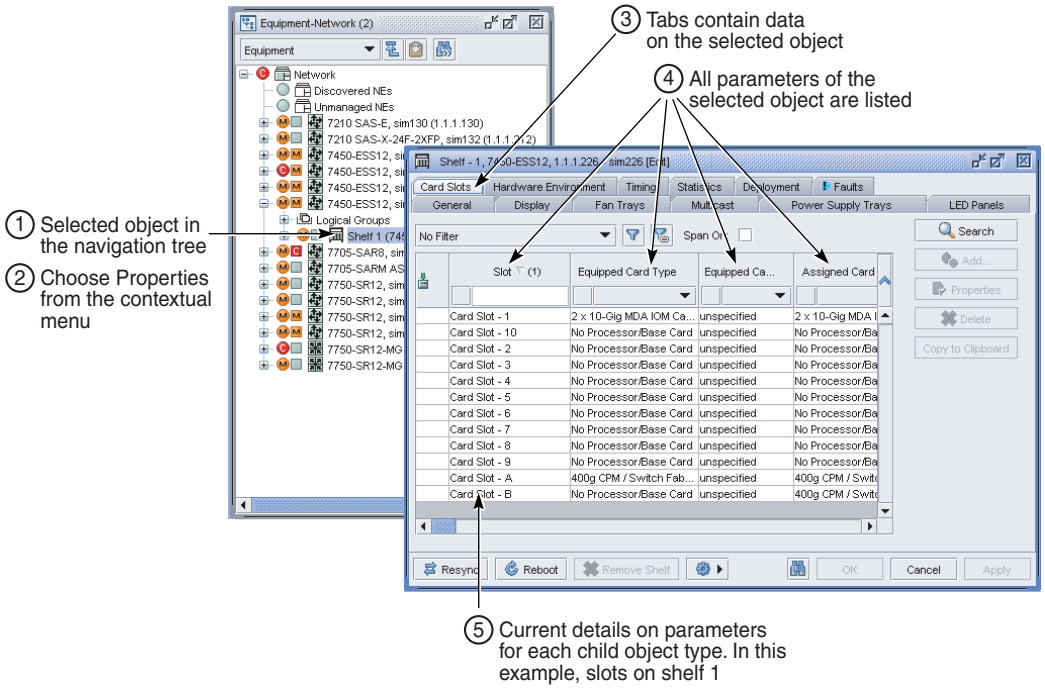


Figure 17-2 shows how to use the properties form for a network object, in this case a shelf on a managed device, to inventory data for the managed device.

Figure 17-2 Generating inventory data for a managed device



Save the data in CSV or HTML format. You can use the saved file for further processing on another platform; for example, as input to a back-office parts management system. Figure 17-3 shows the output of an inventory list saved in CSV format.

Figure 17-3 CSV inventory output

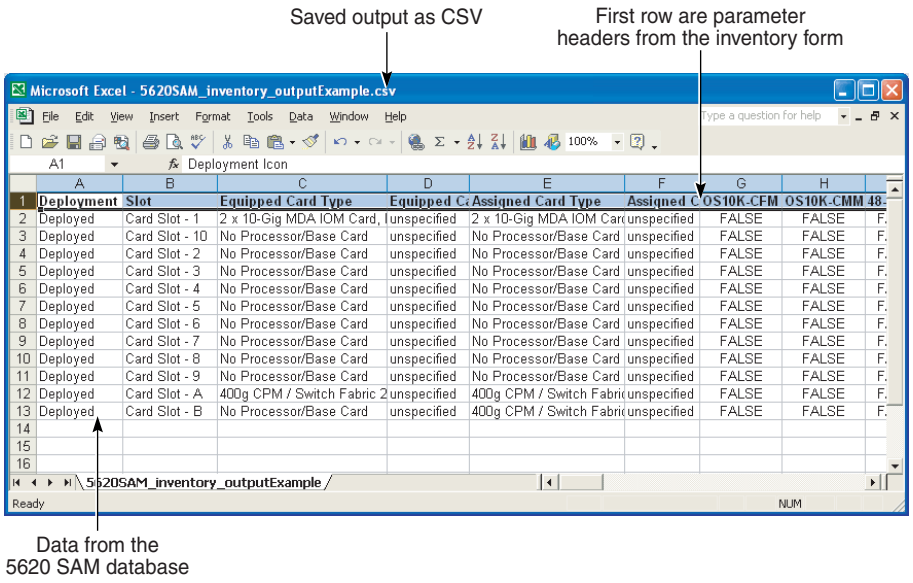
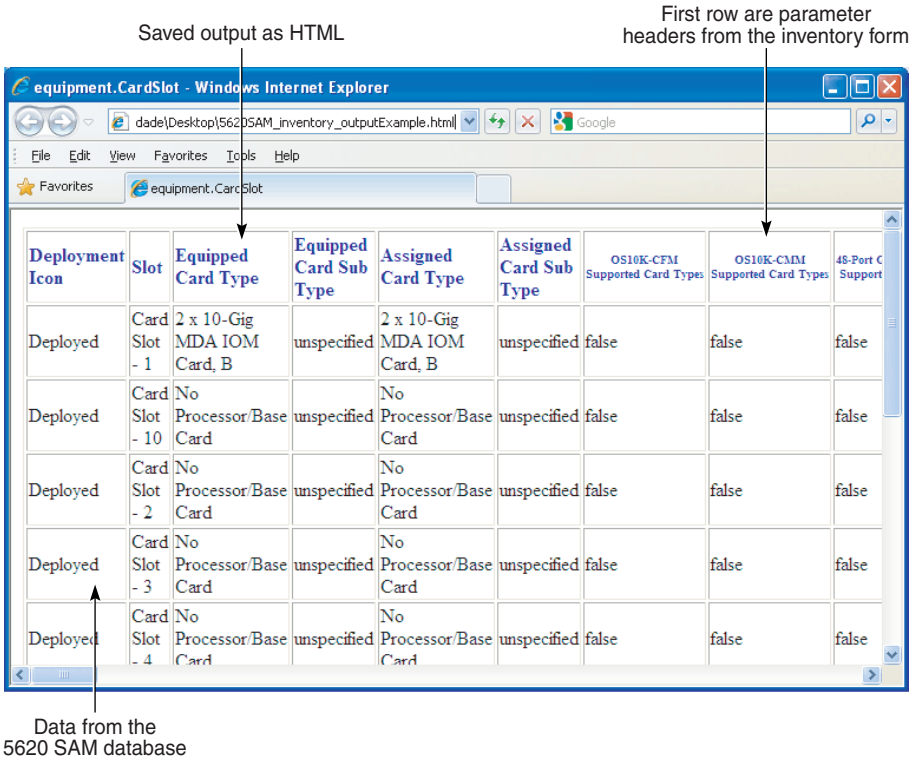


Figure 17-4 shows the output of an inventory list saved in HTML format.

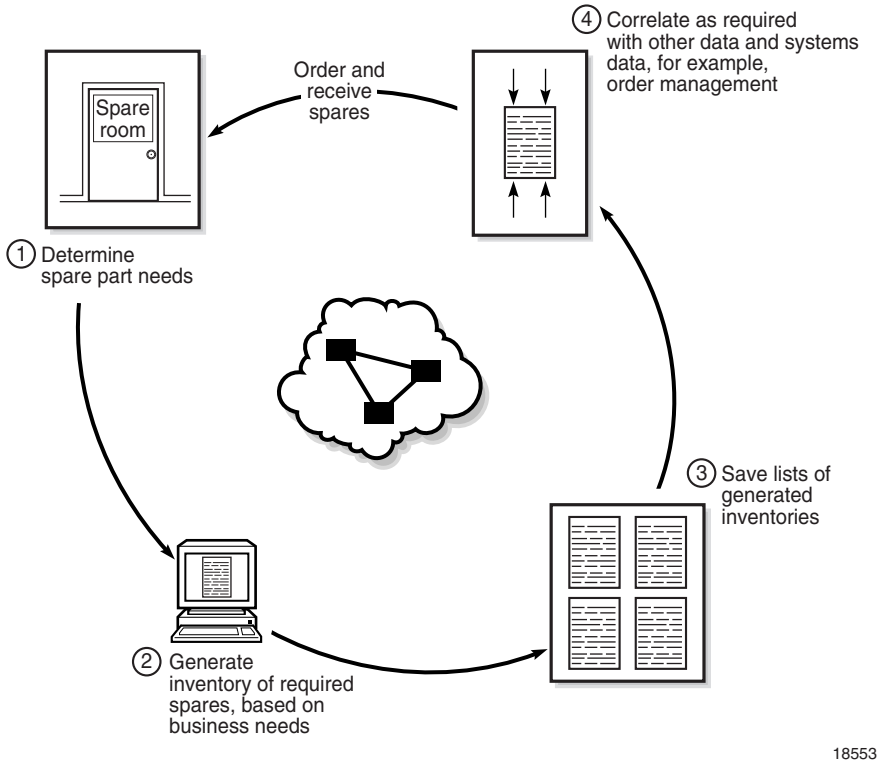
Figure 17-4 HTML inventory output



17.2 Sample inventory management workflow

Figure 17-5 shows an example of an inventory management workflow using the client GUI to generate a list of required spare parts, based on business needs.

Figure 17-5 Example of an inventory management workflow



This example is configured using the following high-level tasks.

1 Determine spare part needs based on business needs and future growth plans.

2 Using the 5620 SAM, generate inventory lists of required spares, keeping in mind the following points.

- Filter the list form to list only those objects that you want; for example, cards of a certain type required for sparing.
- Generate multiple lists, based on business needs.

3 Using the 5620 SAM, save lists of required spares in a format compatible with your back-office systems; for example, CSV or HTML. Move the lists to another system, as required by the back-office applications; for example, an order management or data management system.

4 Correlate inventory lists with data from other back-office systems, as required by business needs.

17.3 Workflow to manage inventory

1. Determine inventory management needs.
2. Provide inventory management list requirements to NOC operators.
3. As required, generate inventory lists for a managed device or for the entire network. See Procedure 17-1 for more information.
4. As required, generate inventory lists for a managed device from the 5620 SAM client GUI:
   - **a** Generate inventory lists for CLEI codes. See Procedure 17-5 for more information.
   - **b** Generate inventory lists for card software versions. See Procedure 17-6 for more information.
   - **c** Generate inventory lists for port types. See Procedure 17-7 for more information.
   - **d** Generate inventory lists for shelf data. See Procedure 17-8 for more information.
5. As required, generate inventory lists for the entire network from the 5620 SAM client GUI:
   - **a** Generate inventory lists for all managed CCMs. See Procedure 17-9 for more information.
   - **b** Generate inventory lists for all managed cards. See Procedure 17-10 for more information.
   - **c** Generate inventory lists for all managed fan trays. See Procedure 17-11 for more information.
   - **d** Generate inventory lists for all managed flash memory. See Procedure 17-12 for more information.
   - **e** Generate inventory lists for all managed physical links. See Procedure 17-13 for more information.
   - **f** Generate inventory lists for all managed ports. See Procedure 17-14 for more information.
   - **g** Generate inventory lists for all managed power supply trays. See Procedure 17-15 for more information.
   - **h** Generate inventory lists for all managed processors. See Procedure 17-16 for more information.
   - **i** Generate inventory lists for all managed shelves. See Procedure 17-17 for more information.

j Generate inventory lists for all management ports. See Procedure 17-18 for more information.

k Generate inventory data for network device SLA audits. See Procedure 17-19 for more information.

6 As required, save search filters. See Procedure 17-4 for more information.

7 As required, save inventory lists in the required formats:

a Save inventory lists in HTML format. See Procedure 17-2 for more information.

b Save inventory lists in CSV format. See Procedure 17-3 for more information.

8 Move inventory lists to other platforms for post-processing.

17.4 Inventory management procedures

Use the following procedures to perform inventory management tasks.

Procedure 17-1 To list and sort inventory data

Perform this procedure to list and sort inventory data for a device or for the entire network.

1 Inventory can be listed and sorted for a device or for the entire network.

a To list and sort inventory for a device, perform steps 2 to 6.

b To list and sort inventory for the entire network, perform steps 7 to 11.

2 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

3 Choose a Network Element (Network) from the object drop-down list and click on the Search button. The list form displays the results of the inventory search.

4 Choose an NE from the list and click on the Properties button. The Network Element (Edit) form opens.

5 Click on the Inventory tab and choose a network object from the object drop-down list. The list form displays the results of the inventory search for the selected device.

6 Go to step 11.

7 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

8 Choose a network object from the object drop-down list.

9 Configure the filter criteria.

10 Click on the Search button. The list form displays the results of the inventory search.

11 Sort the results.

a To count the number of items in the list, generate an inventory of data and right-click on the list heading. The Count shows the number of objects in the list.

b To sort in ascending or descending order, click on the column heading. The arrow direction changes to indicate the order in which the data is sorted.

c To move a column, click on the column, drag the column to the right or left, and drop the column in its new location.

d To remove a column,

i Right-click on the column heading and choose Column Display from the contextual menu. The Column Display window appears.

ii In the Displayed on Table list box, choose the columns that you need to remove from the table and click the left arrow. The specified columns are moved to the Available for Table list box.

iii Click on the OK button to apply the changes and close the Column Display window. The specified columns are removed from the table.

e To sort multiple columns, right-click on a column heading and choose Show Sorting from the contextual menu. The Show Sorting form opens. Choose the property or properties from the Available for Sorting panel and click on the right arrow button. The property or properties appear in the Used for Sorting panel. Click on the Sort Ascending or Sort Descending button, as required.

12 Save the inventory output by performing Procedure 17-2 or 17-3.

13 Close the form.

Procedure 17-2 To save inventory output in HTML format

1 Define the filter properties for the inventory search, and list and sort the output as described in Procedure 17-1.

2 Right-click on a column heading of the inventory output and choose Save to File from the contextual menu. The Save form opens.

3 Save the inventory output.

i To choose a directory in which to save the listed information, use the Save In parameter.

ii To create a filename, use the File Name parameter.

iii Choose HTML (*.htm, *.html) from the Files of Type drop-down menu.

iv Click on the Save button. The results of the inventory search are saved to the specified HTML file.

4 Close the form.

Procedure 17-3 To save inventory output in CSV format

1 Define the filter properties for the inventory search, and list and sort the output as described in Procedure 17-1.

2 Right-click on a column heading of the inventory output and choose Save to File from the contextual menu. The Save form opens.

3 Save the inventory output.

i To choose a directory in which to save the listed information, use the Save In parameter.

ii To create a filename, use the File Name parameter.

iii Choose CSV (*.csv) from the Files of Type drop-down menu.

iv Click on the Save button. The results of the inventory search are saved to the specified CSV file.

4 Close the form.

Procedure 17-4 To save a filter

See Procedure 3-33 for more information.

Procedure 17-5 To inventory CLEI codes for managed device objects

1 You can list CLEI codes for card slots, cards, daughter card slots and daughter cards.

a To view CLEI codes for a device, perform steps 2 to 7.

b To view CLEI codes for the entire network, perform steps 8 to 13.

2 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

3 Choose a Network Element (Network) from the object drop-down list and click on the Search button. The list form displays the results of the inventory search.

4 Choose an NE from the list and click on the Properties button. The Network Element (Edit) form opens.

5 Click on the Inventory tab and choose a network object from the object drop-down list. For example:

- To display the cards and daughter cards that are configured in the slots, expand Slot (Physical Equipment and select one of the following:
  - Card Slot (Physical Equipment)
  - Daughter Card Slot (Physical Equipment)
- To display the IOMs that are installed on, pre-provisioned, or provisioned for the NE, expand Card (Physical Equipment) select IO Card (Physical Equipment)

In each instance, the list form displays the results of the inventory search for the selected device.

6 To obtain a list of CLEI codes for the network object selected in step 5, perform step 11d of Procedure 17-1 to remove all columns from the list except for the object ID or object type and the CLEI code columns.

7 Go to step 12.

8 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

9 Choose a network object from the object drop-down list.

10 Click on the Search button. The list form displays the results of the inventory search.

11 To obtain a list of CLEI codes for the network object selected in step 5, perform step 11d of Procedure 17-1 to remove all columns from the list except for the site ID, object ID, and CLEI code columns

12 Save the CLEI code inventory output.

a To save the results in HTML format, perform steps 2 and 3 of Procedure 17-2.

b To save the results in CSV format, perform steps 2 and 3 of Procedure 17-3.

13 Close the form.

Procedure 17-6 To inventory card software versions for a managed device

You can inventory card software versions for a managed device.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Network Element (Network) from the object drop-down list.

3 Click on the Search button. The list form displays the results of the inventory search.

4 Choose an NE from the list and click on the Properties button. The Network Element (Edit) form opens.

5 Click on the Inventory tab and choose Card (Physical Equipment) from the object drop-down list. The list form displays the results of the inventory search.

6 To obtain a list of card software versions for the selected device, perform step 11d of Procedure 17-1 to remove all columns from the list except for the following:

- Slot ID
- Software Version

7 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 17-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 17-3.

8 Close the form.

Procedure 17-7 To inventory port types for a managed device

Perform this procedure to generate an inventory of port types, such as physical ports, SONET channels, link aggregation groups, terminations, TDM channels, protocols, multilink bundles, and APS groups.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Network Element (Network) from the object drop-down list.

3 Click on the Search button. The list form displays the results of the inventory search.

4 Choose an NE from the list and click on the Properties button. The Network Element (Edit) form opens.

5 Click on the Inventory tab and choose Port (Physical Equipment) from the object drop-down list. The list form displays the results of the inventory search.

6 To display more detailed port inventory information expand to the following sub-objects on the object drop-down list:

- SONET Channels
- Link Aggregation Groups
- TDM Channels
- Multilink Bundles
- APS Groups

7 To sort the inventory output, perform step 11 of Procedure 17-1.

8 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 17-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 17-3.

9 Close the form.

Procedure 17-8 To inventory shelf data for a managed device

Perform this procedure to generate an inventory of shelf manufacturer information, part numbers, serial numbers, CLEI codes, and CLLI codes for the shelves of a managed device.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Network Element (Network) from the object drop-down list.

3 Click on the Search button. The list form displays the results of the inventory search.

4 Choose an NE from the list and click on the Properties button. The Network Element (Edit) form opens.

5 Click on the Inventory tab and choose Shelf (Physical Equipment) from the object drop-down list. The list form displays the results of the inventory search.

6 Choose a shelf from the list and click on the Properties button. The Shelf (Edit) form opens with the General tab displayed.

7 Click on the Display tab. A picture of the selected shelf is displayed.

8 Use screen capture software to record the screen image, or otherwise copy the shelf information to a file for further processing.



Note — You can generate an inventory of shelf data for the managed network, but not for an individual managed devices. See Procedure 17-17 for more information.

9 Close the form.

Procedure 17-9 To inventory all managed CCMs

You can inventory all managed CCMs in a network of managed devices.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose CCM (Physical Equipment) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 To obtain a list of CCM-specific codes, perform step 11d of Procedure 17-1 to remove all columns from the list except for the following:

- Manufacture Date
- Part Number
- Serial Number
- CLEI Code
- CCM Index
- CCM Equipped Type

6 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 17-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 17-3.

7 Close the form.

Procedure 17-10 To inventory all managed cards

You can inventory all managed cards in a network of managed devices.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Card (Physical Equipment) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 To obtain a list of card-specific codes, perform step 11d of Procedure 17-1 to remove all columns from the list except for the following:

- Manufacture Date
- Part Number
- Serial Number
- CLEI Code

6 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 17-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 17-3.

7 Close the form.

Procedure 17-11 To inventory all managed fan trays

You can inventory all managed fan trays in a network of managed devices.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Fan Tray (Physical Equipment) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 To obtain a list of fan tray-specific codes, perform step 11d of Procedure 17-1 to remove all columns from the list except for the following:

- Operational State
- Administrative State
- Device State

6 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 17-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 17-3.

7 Close the form.

Procedure 17-12 To inventory all managed flash memory

You can inventory all managed flash memory in a network of managed devices.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Flash Memory (Physical Equipment) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 To obtain a list of flash memory-specific codes, perform step 11d of Procedure 17-1 to remove all columns from the list except for the following:

- Serial Number
- Firmware Revision
- Model Number
- Capacity (sectors)
- Amount Used (sectors)

6 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 17-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 17-3.

7 Close the form.

Procedure 17-13 To inventory all managed physical links

You can inventory all managed physical links in a network of managed devices.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Physical Link (Network) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 To obtain a list of physical link-specific codes, perform step 11d of Procedure 17-1 to remove all columns from the list except for the following:

- Endpoint A Type
- Endpoint A - Port
- Endpoint B Type
- Endpoint B - Port

6 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 17-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 17-3.

7 Close the form.

Procedure 17-14 To inventory all managed ports

You can inventory all managed ports in a network of managed devices.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Port (Physical Equipment) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 To obtain a list of port-specific codes, perform step 11d of Procedure 17-1 to remove all columns from the list except for the following:

- Name
- CLI Name
- MTU (bytes)
- State

6 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 17-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 17-3.

7 Close the form.

Procedure 17-15 To inventory all managed power supply trays

You can inventory all managed power supply trays in a network of managed devices.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Power Supply Tray (Physical Equipment) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 To obtain a list of power supply tray-specific codes, perform step 11d of Procedure 17-1 to remove all columns from the list except for the following:

- Administrative State
- Operational State
- AC Voltage Status
- DC Voltage Status
- Assigned Type

6 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 17-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 17-3.

7 Close the form.

Procedure 17-16 To inventory all managed processors

You can inventory all managed processors in a network of managed devices.



Note — The eNodeB, 9471 WMM, and 5780 DSC have distinct types of control cards. See "General NE management" in the *5620 SAM LTE RAN User Guide* for information about performing inventory tasks for the eNodeB. See "9471 WMM configuration management" and "Viewing 5780 DSC properties" in the *5620 SAM LTE EPC User Guide* for information about performing inventory tasks for the 9471 WMM and 5780 DSC.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Processor (Physical Equipment) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 To obtain a list of processor-specific codes, perform step 11d of Procedure 17-1 to remove all columns from the list except for the following:

- Operational State
- Administrative State
- CLEI Code
- Manufacturer
- Manufacture Date
- Part Number
- Serial Number

6 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 17-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 17-3.

7 Close the form.

Procedure 17-17 To inventory all managed shelves

You can inventory all managed shelves in a network of managed devices.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Shelf (Physical Equipment) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 To obtain a list of shelf-specific codes, perform step 11d of Procedure 17-1 to remove all columns from the list except for the following:

- Operational State
- Administrative State
- CLEI Code
- Manufacturer
- Manufacture Date
- CLLI Code
- Part Number
- Serial Number (Manufacturer Details)

6 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 17-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 17-3.

7 Close the form.

Procedure 17-18 To inventory all management ports

You can inventory all management ports in a network of managed devices.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Network Element (Network) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 To obtain a list of management port-specific codes, perform step 11d of Procedure 17-1 to remove all columns from the list except for the following:

- System ID
- Management IP Address
- Location
- Chassis Type
- Sys Object ID
- Software Version
- Descriptor Version (software release)
- Resource Group ID

6 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 17-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 17-3.

7 Close the Manage Equipment form.

Procedure 17-19 To collect inventory data for network device SLA audits

You can create lists of inventory data to provide the specific summary information required for SLA audits. Ensure the following before you start:

- Inventory collection requirements differ based on SLA agreements. Ensure that the correct data is being collected for your SLA agreement.
- Perform inventory collection during a maintenance window, or during low network activity windows to ensure no impact to systems.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Collect the required SLA audit data.

a For card SLA audits, choose Card (equipment) from the object drop-down list.

b For shelf SLA audits, choose Shelf (equipment) from the object drop-down list.

c For power supply tray SLA audits, choose Power Supply Tray (equipment) from the object drop-down list.

3 Click on the Search button. The SLA audit data appears in the list.

4 Typically, only a subset of data is required for SLA audits. To display only the required information, perform the following:

i Left-click on the list column heading. The list contextual menu appears.

ii Ensure the information that you want displayed has a check mark. These typically include:

- Identification information, such as Site ID, Site Name, Slot ID, and Slot Name
- SLA audit and ordering information, such as Manufacture Date, Part Number, Serial Number, CLEI Code, and Card Type

iii Close the list contextual menu. Only the chosen information is displayed in the list.

iv Choose Save Table Preferences from the list contextual menu to save the refined list for future use. When a similar search from the same client GUI is performed, the refined list is shown by default.

v Confirm the action.

5 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 17-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 17-3.

6 Close the form.

18 — Card migration

18.1 Card migration management overview *18-2*

18.2 Workflow to manage card migration *18-3*

18.3 Card migration management procedures *18-4*

18.1 Card migration management overview

You can use a 5620 SAM GUI utility called the Card Migration Event Manager to facilitate the transition to an IOM 3 on one or more 7450 ESS or 7750 SR NEs. The Card Migration Event Manager transfers the existing IOM and MDA configurations to new modules with minimal service interruption.

The 5620 SAM Card Migration Event Manager can do the following:

- Upgrade from an IOM 1 or IOM 2 to an IOM3 while retaining the same MDAs.
- Upgrade from one MDA type to a newer MDA type that has compatible features.
- Upgrade an IOM and the associated MDAs in one operation.

You can perform an immediate migration, or preconfigure one or more migration events for later execution. A migration event can include an NE reboot to put the new hardware configuration into effect immediately after the migration. You can upgrade multiple IOMs and MDAs in one operation to limit the number of required NE reboots to one.

During a migration event, the 5620 SAM identifies the configured objects that are bound to the IOM or MDA, deletes the objects, and then creates the objects on the new IOM or MDA. The old and new configurations are saved in the 5620 SAM database until the migration completes successfully. The 5620 SAM preserves the statistics data and alarm information that is associated with each object.

Restrictions

The following restrictions apply to 5620 SAM card migration event management:

- **General**
  - Only the 5620 SAM admin user, or a user with an assigned administrator scope of command role, can create, modify, or execute a migration event.
  - The migration functions are not available to 5620 SAM OSS clients.
  - You may need to re-enable SNMP on an NE after the NE reboots following a migration event.
  - You can only perform a card migration if the description associated with the cards being migrated do not contain any numerical values.
- **IOM-specific**
  - An IOM downgrade, for example, a migration from an IOM 3 to an IOM 2, is not supported.
- **MDA-specific:**
  - You cannot migrate an empty MDA slot to an MDA.
  - MDA migration is limited to MDAs of the same physical transmission type; for example, migration from a SONET MDA to an Ethernet MDA is not supported.
  - You cannot upgrade an MDA that is integrated with an IOM, for example, an IMM.
  - For MDAs, you can migrate only to an MDA of similar capacity that has the same or a greater number of ports.

The 5620 SAM raises an alarm during a migration event if a target NE is unreachable. After a migration event, the 5620 SAM raises an alarm to indicate migration success or failure.

Table 18-1 lists the supported MDA migration types.

Table 18-1 Supported MDA migration types

Current MDA	MDAs supported by migration
10 x 1-Gig Ethernet SFP	10 x 1Gig Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
5 x 1-Gig Ethernet SFP	10 x 1Gig Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
1 x 10-Gig Ethernet	4 x 10Gig Extended Performance XFP 2 x 10Gig Extended Performance XFP 1 x 10Gig Extended Performance SFP
20 x 100 Ethernet Fx	20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
20 x 10/100/1000 Ethernet Tx	20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
2 x 10-Gig Ethernet XFP	2 x 10Gig Extended Performance XFP 4 x 10Gig Extended Performance XFP
20 x 10/100/1000 Ethernet SFP	20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
1 x 10-gig Ethernet XFP	4 x 10GigExtended Performance XFP 2 x 10Gig Extended Performance XFP 1 x 10Gig Extended Performance XFP
5 x 10/100/1000	10 x 1Gig Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
10 x 10/100/1000 Ethernet SFP	10 x 1Gig Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
60 x 10/100 Ethernet	48 x 10/100/1000 Ethernet Extended Performance TX

18.2 Workflow to manage card migration

The following is the sequence of high-level actions required to manage card migration.

1 Use the 5620 SAM to back up the device configuration of each target NE.



Note — When you attempt a migration on an NE that does not have a recent configuration backup in the 5620 SAM database, the 5620 SAM raises an alarm and the migration fails.

A recent configuration backup is a backup that occurs after the latest configuration save on the NE.

See “NE maintenance” in the *5620 SAM System Administrator Guide* for information about performing NE backups.

2 Create a card migration event and execute or save it, as required. See Procedure 18-1 for more information.

3 Execute a saved card migration event, as required. See Procedure 18-2 for more information.

18.3 Card migration management procedures

Use the following procedures to perform card migration event management tasks.

Procedure 18-1 To create a card migration event

1 Choose Tools→Card Migration Event Manager from the 5620 SAM main menu. The Card Migration Event Manager form opens.

2 Click on the Create button. The Card Migration Event (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Description
- Additional Information
- Auto Reboot

4 Click on the NE Migration Candidates tab.

5 Click on the Add button. The Select Network Elements - Card Migration Event form opens.

6 Select one or more NEs in the list and click on the OK button. The Select Network Elements - Card Migration Event form closes and the NEs are listed on the Card Migration Event (Create) form.

7 Select one or more NEs in the list and click on the Properties button. The Network Element Migration Candidates form opens.

8 Configure the Auto Reboot parameter.

9 Click on the Ok button. The Network Element Migration Candidates form closes, and a dialog box appears.

10 Click on the OK button.

11 Click on the Card Migration Candidates tab.

12 Click on the Add button. The Select Cards - Card Migration Event form opens.

13 Select one or more cards in the list and click on the OK button. The Select Cards - Card Migration Event form closes and the cards are listed on the Card Migration Event (Create) form.

14 Select one or more cards in the list and click on the Properties button. The Migration Details (Create) form opens.

15 Configure the New Type parameter in the IOM panel, if required.

16 Configure the New Type parameter in the MDA 1 panel, if required.

17 Configure the New Type parameter in the MDA 2 panel, if required.

18 Click on the OK button. The Migration Details (Create) form closes, and a dialog box appears.

19 Click on the OK button.

20 To execute the migration event immediately, perform the following steps. Otherwise, you can execute the migration later by performing Procedure 18-2.

i Use the 5620 SAM to back up the device configuration of each target NE.



Note — When you attempt a migration on an NE that does not have a recent configuration backup in the 5620 SAM database, the 5620 SAM raises an alarm and the migration fails.

A recent configuration backup is a backup that occurs after the latest configuration save on the NE.

ii Click on the Apply button. The 5620 SAM saves the card migration event configuration.

iii Click on the General tab to display the Status indicator.

iv Click on the Initiate Migration button. A dialog box appears.

v Click on the Yes button. The 5620 SAM starts to migrate the specified cards.

vi Monitor the card migration as it progresses by viewing the Status indicator on the form. The status can be one of the following:

- Awaiting manual reboot to complete migration
- Failed - Latest configuration not available
- Failed - Unable to migrate configuration
- Failed - Unable to reboot network element
- Failed - Unable to transfer migrated configuration
- Migration completed
- Not Started
- Rebooted network element
- Started
- Swap failed
- Swap failed on some network elements

21 Click on the OK button. The Card Migration Event (Create) form closes.

22 Close the Card Migration Event Manager form.

Procedure 18-2 To execute a saved card migration event

1 Use the 5620 SAM to back up the device configuration of each target NE.



Note — When you attempt a migration on an NE that does not have a recent configuration backup in the 5620 SAM database, the 5620 SAM raises an alarm and the migration fails.

A recent configuration backup is a backup that occurs after the latest configuration save on the NE.

2 Choose Tools→Card Migration Event Manager from the 5620 SAM main menu. The Card Migration Event Manager form opens.

3 Configure the filter criteria and click on the Search button. A list of card migration events is displayed.

4 Select a card migration event and click on the Properties button. The Card Migration Event (Edit) form opens with the General tab displayed.

5 Click on the Initiate Migration button. A dialog box appears.

6 Click on the Yes button. The 5620 SAM starts to migrate the specified cards.

7 Monitor the card migration as it progresses by viewing the Status indicator on the form. The status can be one of the following:

- Awaiting manual reboot to complete migration
- Failed - Latest configuration not available
- Failed - Unable to migrate configuration
- Failed - Unable to reboot network element
- Failed - Unable to transfer migrated configuration
- Migration completed
- Not Started
- Rebooted network element
- Started
- Swap failed
- Swap failed on some network elements

8 Click on the OK button. The Card Migration Event (Create) form closes.

9 Close the Card Migration Event Manager form.

Procedure 18-3 To delete a card migration event

1 Choose Tools→Card Migration Event Manager from the 5620 SAM main menu. The Card Migration Event Manager form opens.

2 Configure the filter criteria and click on the Search button. A list of card migration events is displayed.

3 Select a card migration event and click on the Delete button. A dialog box appears.

4 Click on the Yes button. The 5620 SAM deletes the card migration event.

5 Close the Card Migration Event Manager form.

19 — TCA

19.1 TCA overview *19-2*

19.2 Workflow to configure TCA *19-4*

19.3 TCA management procedures *19-4*

19.1 TCA overview

You can create policies to raise 5620 SAM alarms based on managed-object statistics. When a statistic counter of an object such as an interface reaches a specified threshold, the 5620 SAM alerts GUI operators using a threshold-crossing alarm, or TCA, based on policy specifications.

A TCA policy includes the following:

- the direction of traffic flow to monitor
- the objects that are associated with the policy
- rules that define properties such as the rising and falling thresholds, and the alarm severity
- custom statistics counters that can be used to monitor statistics based on specified formulas



Note — A TCA is not self-clearing. The 5620 SAM clears a TCA only when the TCA policy contains a falling-threshold rule in addition to a rising-threshold rule, and the alarm severity in the falling-threshold rule is set to cleared.

To enable TCA on an object, you must enable collection of performance statistics on the object. To determine whether a specified statistic exceeds a TCA policy threshold, the 5620 SAM compares the utilization value at each statistics collection to the threshold values in the associated TCA policy.

The 5620 SAM TCA function raises an alarm when a statistic threshold is initially crossed. Rather than raise a new alarm for each successive threshold-crossing event associated with a TCA policy, the 5620 SAM changes the severity of the initial alarm based on the rules defined in the policy.

In the 5620 SAM client GUI, you can associate a TCA policy with a managed object from the TCA policy configuration form, or from the object properties form. You can associate one TCA policy with multiple objects.

Statistics counters

Depending on the monitored object, you can create rules to monitor utilization, packets in error, and packets dropped.

The 5620 SAM allows you to monitor custom TCA statistics. You can create a custom TCA profile and build a formula using statistics counters and constant values. See “Accounting statistics collection” in the *5620 SAM Statistics Management Guide* for more information on statistics counters.

For all statistics counters, you can choose to apply the rule to the delta value, rather than the absolute value. The delta value is the difference between the current value and most recent previous value of the statistic counter.

TCA configuration example

The following example describes the 5620 SAM configuration required to raise a TCA, adjust the alarm severity, and clear the alarm, based on the following utilization specifications:

- Raise a minor alarm if utilization is between 60% and 69%.
- Change the alarm severity to major if utilization rises to between 70% and 79%.
- Change the alarm severity to critical if utilization rises to 80% or higher.
- Change the alarm severity to major if utilization falls below 80%.
- Change the alarm severity to minor if utilization falls below 70%.
- Clear the alarm if utilization falls below 60%.

The following are the TCA rules and associated parameter values required to implement the example alarm behavior:

Rule to raise minor alarm for 60% or higher utilization:

- Alarm Severity—minor
- Threshold (%)—60
- Threshold Direction—Rising Above

Rule to change alarm severity to major for 70% or higher utilization:

- Alarm Severity—major
- Threshold (%)—70
- Threshold Direction—Rising Above

Rule to change alarm severity to critical for 80% or higher utilization:

- Alarm Severity—critical
- Threshold (%)—80
- Threshold Direction—Rising Above

Rule to change alarm severity to major if utilization falls below 80%:

- Alarm Severity—major
- Threshold (%)—80
- Threshold Direction—Falling Below

Rule to change alarm severity to minor if utilization falls below 70%:

- Alarm Severity—minor
- Threshold (%)—70
- Threshold Direction—Falling Below

Rule to clear alarm if utilization falls below 60%:

- Alarm Severity—cleared
- Threshold (%)—60
- Threshold Direction—Falling Below

19.2 Workflow to configure TCA

Perform these steps to configure a TCA policy on a monitored object.

1 Enable performance statistics collection on the object that is to be monitored. For example, Table 19-1 lists the port statistics policy objects required to enable TCA on a network interface or physical link.

Table 19-1 Port statistics policy objects for TCA

Statistics policy type	MIB	MIB entry	Monitored class
NE MIB	IF-MIB	ifEntry	—
Specific MIB	IF-MIB	ifEntry	equipment.PhysicalPort
Interface Additional Stats	IF-MIB	ifXEntry	lag.Interface

See "Performance statistics collection" in the *5620 SAM Statistics Management Guide* for more information about collecting performance statistics.

2 If you are creating custom TCA rules, configure a custom TCA profile. See Procedure 19-1 for more information.

3 Configure a TCA policy. See Procedure 19-2 for more information.

- **i** Configure a TCA policy.
- **ii** Configure utilization, error, and drop TCA rules.
- **iii** If required, configure custom TCA rules using custom TCA profiles.

4 Apply a TCA policy to an object. See Procedure 19-3 for more information.

5 As required, customize the TCA system preferences associated with TCA policies such as specifying the default TCA alarm severity or the maximum TCA alarm limit. See "System preferences configuration procedures" in the *5620 SAM System Administrator Guide* for more information about customizing TCA system preferences.

6 As required, delete a TCA policy. See Procedure 19-4 for more information.

19.3 TCA management procedures

The following procedures describe how to manage TCA policies.

Procedure 19-1 To configure a custom TCA profile

Perform this procedure to create a custom TCA profile to apply to a TCA policy.

1 Choose Tools→TCA Policies from the 5620 SAM main menu. The TCA Policies form opens.

2 Choose CustomProfileTCA (TCA Policy) from the object type drop-down menu.

3 Click on the Create button. The CustomProfileTCA (Create) form opens.

4 Configure the parameters:

- Profile ID
- Auto-Assign ID
- Profile Name
- Description

5 Click on the Select button. The Custom Profile TCA (Create) form opens.

6 Configure the filter criteria, if required, and click on the Search button.

7 Select a monitored object from the list and click on the OK button. The Custom Profile TCA (Create) form closes.

8 Configure the Stats Type parameter.

9 Click on the Build Formula button. The Build Formula form opens.

10 Choose a statistic counter from the Counter Field drop-down menu.

11 Click on the Add button.

12 Add as many expressions to the formula as required.

a Add a statistic counter to the formula.

i Click on one of the mathematical operator buttons.

ii Choose a counter from the Counter Field drop-down menu.

iii Click on the Add button.

b Add a constant value to the formula.

i Click on one of the mathematical operator buttons.

ii Enter a number in the Constant Value field.

iii Click on the Add button.

13 Click on the OK button. The Build Formula form closes.

14 Click on the OK button. The CustomProfileTCA (Create) form closes.

15 Close the TCA Policies form.

Procedure 19-2 To configure a TCA policy

Perform this procedure to configure a TCA policy for monitoring object utilization.

1 Choose Tools→TCA Policies from the 5620 SAM main menu. The TCA Policies form opens.

2 Choose TCAPolicy (TCA Policy) from the object type drop-down menu.

3 Click on the Create button. The TCAPolicy (Create) form opens.

4 Configure the parameters:

- Policy ID
- Auto-Assign ID
- Displayed Name
- Description
- TCA Admin State

5 Click on the Select button. The TCAPolicy form opens.

6 Configure the filter criteria, if required, and click on the Search button.

7 Select a monitored object from the list and click on the OK button. The TCAPolicy form closes.

8 Click on the Apply button. The TCAPolicy (Create) form closes and the TCAPolicy (Edit) form opens with the General tab displayed.



Note — The panels that appear on the General tab depend on which object type you are creating a TCA policy for.

9 If applicable, configure utilization TCA rules.

i In the Utilization panel, configure the parameters:

- Disable TCA
- Flow Direction
- Delta Tolerance

ii Click on the Create button in the Rules subpanel. The PercentageTCARule, tca.UtilizationTCA-0 (Create) form opens.

iii Configure the parameters:

- Rule ID
- Auto-Assign ID
- Displayed Name
- Alarm Severity
- Threshold (%)
- Threshold Direction
- Use for Delta TCA

iv Click on the OK button. The PercentageTCARule, tca.UtilizationTCA-0 (Create) form closes.

v Repeat steps ii to iv to create additional rules, as required.



Note — You cannot create two rules that have the same Threshold (%) and Threshold Direction values.

10 If applicable, configure error TCA rules.

i In the Error panel, configure the parameters:

- Disable TCA
- Flow Direction
- Delta Tolerance

ii Click on the Create button in the Rules subpanel. The PercentageTCARule, tca.ErrorTCA-0 (Create) form opens.

iii Configure the parameters:

- Rule ID
- Auto-Assign ID
- Displayed Name
- Alarm Severity
- Threshold (%)
- Threshold Direction
- Use for Delta TCA

iv Click on the OK button. The PercentageTCARule, tca.ErrorTCA-0 (Create) form closes.

v Repeat steps ii to iv to create additional rules, as required.



Note — You cannot create two rules that have the same Threshold (%) and Threshold Direction values.

11 If applicable, configure drop TCA rules.

i In the Drop panel, configure the parameters:

- Disable TCA
- Flow Direction
- Delta Tolerance

ii Click on the Create button in the Rules subpanel. The PercentageTCARule, tca.DropTCA-0 (Create) form opens.

iii Configure the parameters:

- Rule ID
- Auto-Assign ID
- Displayed Name
- Alarm Severity
- Threshold (%)
- Threshold Direction
- Use for Delta TCA

iv Click on the OK button. The PercentageTCARule, tca.DropTCA-0 (Create) form closes.

v Repeat steps ii to iv to create additional rules, as required.



Note — You cannot create two rules that have the same Threshold (%) and Threshold Direction values.

12 If applicable, configure custom TCA rules.

i In the Custom panel, click on the Create button. The CustomTCA (Create) form opens.

ii Configure the parameters:

- ID
- Auto-Assign ID
- Disable TCA
- Displayed Name
- Delta Tolerance

iii Click on the Select button. The Select Custom Profile TCA - CustomTCA form opens.

iv Configure the filter criteria, if required, and click on the Search button.

v Select a Custom TCA Profile from the list and click on the OK button. The Select Custom TCA Profile - CustomTCA form closes.

vi Click on the Create button in the Rules panel. The CustomTCARule, tca.CustomTCA-0 (Create) form opens.

vii Configure the parameters:

- Rule ID
- Auto-Assign ID
- Displayed Name
- Alarm Severity
- Threshold
- Delta Threshold (%)
- Threshold Direction
- Use for Delta TCA

viii Click on the OK button. The CustomTCARule, tca.CustomTCA-0 (Create) form closes.

ix Click on the OK button. The CustomTCA (Create) form closes and a dialog box opens.

x Click on the OK button.

13 Apply the TCA Policy to monitored objects, as required.

i Click on the Monitored Objects tab.

ii Click on the Add button. The Select form opens.

iii Configure the filter criteria, if required, and click on the Search button.

iv Select one or more objects from the list and click on the OK button. The Select form closes.

14 Click on the OK button. A dialog box opens.

15 Click on the OK button to confirm the changes. The TCAPolicy (Edit) form closes.

16 Close the TCA Policies form.

Procedure 19-3 To apply a TCA policy to objects using the object properties forms

Perform this procedure to apply an existing TCA policy to an object from the object properties form.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Select an object from the Select Object Type drop-down menu.

3 Configure the filter criteria, if required, and click on the Search button.

4 Select an object from the list and click on the Properties button. The properties form for the object opens.

5 If the object is a Physical Link, perform the following steps.

i Click on the End Point A TCA tab.

ii Click on the Assign button. The Select TCA Policy form opens.

iii Configure the filter criteria, if required, and click on the Search button.

iv Select a TCA policy in the list and click on the OK button. The Select TCA Policy form closes and the TCA policy is listed on the object properties form.

v Click on the End Point B TCA tab.

vi Click on the Assign button. The Select TCAPolicy form opens.

vii Configure the filter criteria, if required, and click on the Search button.

viii Select a TCA policy in the list and click on the OK button. The Select TCA Policy form closes and the TCA policy is listed on the object properties form.

ix Go to step 10.

6 Click on the TCA tab.

7 Click on the Assign button. The Select TCAPolicy form opens.

8 Configure the filter criteria, if required, and click on the Search button.

9 Select a TCA policy in the list and click on the OK button. The TCA policy is listed on the object properties form.

10 Close the object properties form.

11 Close the Manage Equipment form.

Procedure 19-4 To delete a TCA policy

Perform this procedure to delete a TCA policy.

1 Choose Tools→TCA Policies from the 5620 SAM main menu. The TCA Policies form opens.

2 Configure the filter criteria, if required, and click on the Search button.

3 Select one or more TCA policies in the list and click on the Delete button. The 5620 SAM deletes the TCA policies.

4 Close the TCA Policies form.

20 — Bulk operations

20.1 Bulk operations overview *20-2*

20.2 Workflow to manage bulk operations *20-2*

20.3 Bulk operations procedures *20-2*

20.1 Bulk operations overview

The 5620 SAM bulk operations function allows you to create bulk changes to modify a large amount of information. Bulk changes may be deployed to NEs or restricted to the 5620 SAM.

A bulk change can contain thousands of target objects. These objects, referred to as batch items, are grouped into batches for efficient bulk change execution. An operator can execute an entire bulk change or individual batches.

You should regenerate batches each time you execute a bulk change to ensure that each target object that matches the bulk change filter is modified.

If one or more of the batch items fail to change during a bulk change operation, the Batch Status and the Batch Status Summary parameters help identify the items. You can also use the Task Manager to view information about a batch.

20.2 Workflow to manage bulk operations

1. Create a bulk change. See Procedure 20-1 for more information.
2. Generate batches for a bulk change. See Procedure 20-3 for more information.
3. Execute one or more batches in a bulk change. See Procedure 20-3 for more information.
4. As required, stop a bulk change. See Procedure 20-5 for more information.
5. View the bulk change execution results to verify that the bulk change was successful and to identify any items which failed to change. See Procedure 20-4 for more information.

20.3 Bulk operations procedures

Use the following procedures to manage 5620 SAM bulk operations.

Procedure 20-1 To create a bulk change

1 Choose Tools→Bulk Operations from the 5620 SAM main menu. The Bulk Operations form opens.

2 Open the Create Bulk Change form by performing one of the following steps.

a Click on the Create button.

b To create a bulk change by copying values from an existing bulk change, perform the following steps.

i Configure the filter criteria and click on the Search button. A list of bulk operations appears.

ii Choose the bulk change from the list and click on the Properties button. The Bulk Change configuration form opens.

iii Click on the Copy button.

3 Configure the parameters, if required:

- Operation ID
- Auto-Assign ID
- Name
- Description
- Admin State
- Object Type

The Operation ID parameter is configurable when the Auto-Assign ID parameter is disabled.

4 Click on the Next button. The Specify the filter form opens.

5 Perform one of the following to specify a filter.

a Create a filter.

i Click on the Attribute drop down and select an option.

ii Click on the Function drop down and select an option.

iii Click on the Value drop down and select or enter an option.

iv Click on the Add to filter icon. The options are displayed in the filter panel.

v Select AND or OR from the Operators drop down option. Repeat steps i to iv to add more options.

vi Click on Save, the Save Filter form opens.

vii Configure the parameters:

- Filter Name
- Description
- Public

viii Click on the Save button. The Save Filter form closes.

b Load a filter.

i Click on the Saved Filters button. The Saved Filters form opens.

ii Select a saved filter in the list and click on the Load button. The Saved Filters form closes and the loaded filter is displayed in the filter panel.

6 Configure the filter criteria, as required and perform the following steps. Creating a filter that contains the attributes that you want to change can limit the number of objects generated for the bulk change.

7 Click on the Count button to determine the number of network objects that are affected based on the filter.

8 Click on the View button to list the target objects. The Filtered List form opens.

9 Click on the Search button. A list of target objects is displayed.

10 Click on the Next button. The Specify the attributes form opens.

11 Double-click on the attribute or attribute group in the attribute tree panel that you want to include in the bulk change. The attribute or attribute group appears in the display panel.

12 If you included an attribute or attribute group that you want to exclude from the bulk change, you can remove it by clicking on the Remove icon in the display panel.

13 Perform one of the following on each listed attribute, as required.

a Enter a value in the attribute field. The drop-down menu changes from Unchanged to Set, which means that the attribute changes to the new value when you execute the bulk change.

b Choose Default from the drop-down menu to specify that the attribute is to change to the default value when you execute the bulk change.

c Choose Clear from the drop-down menu. Depending on the object type, the attribute value is cleared or set to the default value when you execute the bulk change.

14 Click on the Next button. The Change review form opens.

15 Configure the parameters, if required:

- Batch Size
- Continue on Failure
- Admin State

16 Click on the Finish button.

17 Select the View the newly created Bulk Change check box to view the bulk change after closing the form, if required.

18 Click on the Close button. The Create Bulk Change form closes.

19 To create more Bulk Changes, repeat steps 2 to 18.

Procedure 20-2 To modify a bulk change

1 Choose Tools→Bulk Operations from the 5620 SAM main menu. The Bulk Operations form opens.

2 Configure the filter criteria and click on the Search button. A list of bulk operations appears.

3 Choose the bulk change from the list and click on the Properties button. The Bulk Change configuration form opens with the Batch Control tab displayed.

4 Click on the Summary tab.

5 Modify the parameters, if required:

- Description
- Batch Size
- Admin State
- Continue on Failure

6 Click on the Spans tab and specify a span, if required.

7 Click on the OK button. The Bulk Change configuration form closes.

8 Close the Bulk Operations form.

Procedure 20-3 To execute a bulk change



Note 1 — You can only execute one bulk change at a time. All other bulk changes are queued.

Note 2 — You can only generate batches for one bulk change at a time.

Note 3 — You cannot generate batches when a bulk change is executing.

1 Choose Tools→Bulk Operations from the 5620 SAM main menu. The Bulk Operations form opens.

2 Configure the filter criteria and click on the Search button. A list of bulk operations appears.

3 Choose the bulk change from the list and perform one of the following.

a If the bulk change contains batches, click on the Execute button to execute all of the batches.



Note — Changes made to the network after the batches were generated are not affected by the bulk change batches.

b If the bulk change does not contain batches, or you want to regenerate the batches, perform the following.

i Click on the Properties button. The Bulk Change configuration form opens.

ii If the Generate Batches button is dimmed, perform the following:

- Click on the Summary tab.
- Set the Admin State parameter to Enable.
- Click on the Batch Summary tab.

iii Click on the Generate Batches button. The batches are generated and listed on the form.

iv To execute only specific batches, choose one or more batches from the list and click on the Execute Selected button.

v To execute all of the batches, click on the Execute All button.

A dialog box appears. You can modify the bulk change confirmation message behavior from the User Preferences form.

4 Click on the Yes button. The 5620 SAM executes the bulk change.

Procedure 20-4 To view executed batch information



Note — You can also use the 5620 SAM Task Manager to view information about a batch.

1 Choose Tools→Bulk Operations from the 5620 SAM main menu. The Bulk Operations form opens.

2 Configure the filter criteria and click on the Search button. A list of bulk operations appears.

3 Choose the bulk change from the list and click on the Properties button. The Bulk Change configuration form opens with the Batch Control tab displayed.

4 Choose a batch from the list.

5 Click on the Properties button. The Bulk Change Batch configuration form opens with the General tab displayed. View general information about the executed batch.

6 Click on the Batch Items tab.

7 Click on the Search button. A list of items that were changed in the batch appears with the status of each batch item.

8 To view the parameters for each batch item, choose a batch item from the list and click on the Properties button.

9 Close all of the forms.

Procedure 20-5 To stop one or more bulk changes

1 Choose Tools→Bulk Operations from the 5620 SAM main menu. The Bulk Operations form opens.

2 Configure the filter criteria and click on the Search button. A list of bulk operations appears.

3 Perform one of the following:

- **a** Choose one or more bulk change to stop from the list.
- **b** Choose one or more batches to stop by performing the following:
  - **i** Choose a bulk change from the list.
  - **ii** Click on the Properties button. A Bulk Change configuration form opens with the Batch Control tab displayed.
  - **iii** Choose one or more batches from the list.

4 Click on the Stop button. A dialog box appears.

5 Click on the Yes button. The bulk change execution stops.

6 Close the forms.

Procedure 20-6 To delete a bulk change

1 Choose Tools→Bulk Operations from the 5620 SAM main menu. The Bulk Operations form opens.

2 Configure the filter criteria and click on the Search button. A list of bulk operations appears.

3 Choose the bulk change that you want to delete from the list and click on the Delete button. A dialog box appears.

4 Click on the Yes button. The bulk changes is removed from the 5620 SAM.

21 — Auto-provision

21.1 Auto-provision overview *21-2*

21.2 Workflow to configure network devices using auto-provision *21-4*

21.3 Auto-provision procedures *21-4*

21.1 Auto-provision overview

Auto-provision provides a way to reuse a proven configuration and apply the configuration to multiple NEs of the same type. This functionality is useful when a large number of similar NEs must be configured. Auto-provision reduces configuration errors and the time to configure each NE. Auto-provision takes advantage of the validations that are executed for every 5620 SAM configuration. When you configure a source NE from a 5620 SAM, the need to troubleshoot configuration problems is reduced.

After a source NE is configured and backed up, an operator can import the source script to the source profile. Alternatively, an operator can add the source script manually to the source profile. From the source profile, a target template can be generated. An operator can import the target template, enter any required changes and deploy the configuration template on a target NE.



Note — To ensure that the CLI syntax remains intact, the target NE must be of the same device and chassis type, and at the same release, as the source NE.

Auto-provision extends configuration to an adjacent 7750 SR to ensure a prompt and reliable exchange of traffic between the devices. When the configuration profile is successfully deployed to a 7705 SAR target device, the operator can generate configuration modules to configure interactions between the target device and the adjacent devices. An operator can make minor changes to some of the attributes on the configuration modules and deploy the configuration modules to create objects on the selected 7750 SR. When modules are configured, the operator can deploy the modules to configure the connection. A VLL service site is created on the 7705 SAR and the adjacent 7750 SR. The 5620 SAM automatically creates SAPs and SDP bindings.

The 5620 SAM supports the generation of SAP and SDP configuration modules. Configuration between the 7705 SAR and the adjacent 7750 SR requires the following:

- Base configuration of the 7750 SR is complete and the 7705 SAR is auto-provisioned.
- Interface-level configuration is sent to the adjacent 7750 SR.
- The uplink port of the auto-provisioned 7705 SAR is configured to communicate with the network interface of the 7750 SR. Only Ethernet network interfaces are supported.
- The 7750 SR must be able to communicate with the adjacent 7705 SAR.
- A LDP interface is created on the same interface.
- A MPLS interface is created when MPLS is enabled. Choose either RSVP hop by hop or TE.
- MLPPP is configured on the 7750 SR when MLPPP is configured on the adjacent 7705 SAR.
- A LSP is configured between the 7750 SR and the 7705 SAR.
- An Ethernet, TDM or ATM endpoint is created on the 7750 SR that corresponds to the SAP on the 7705 SAR.

The velocity script generator parses a validated source NE configuration so that the NE is compatible with the velocity script management tool that is available in the 5620 SAM. After the layers are identified, the velocity script generator identifies attributes that require configuration before they can be applied to a target NE. Table 21-1 lists the layers that are identified by the velocity script generator. An operator can add, remove, modify, or hide any of the attributes that are listed. The layers must be configured to deploy together.

Table 21-1 Layers and attributes identified by the velocity script generator

Layer	Attributes
Base Equipment layer	SNMP packet size and daughter cards
Channelization layer	SONET SDH paths and channel groups
Policies layer	QoS and ACL related policies
Routing layer	Routing interface configurations and static routes
Routing Protocols layer	Routing Protocol configurations
MPLS layer	Targeted LDP, MPLS interfaces, and LSPs
Service layer	VLL services including Apipe, Cpipe, Epipe, Ipipe, VPRN, SAP, and SDP bindings



Warning — Scripts that are modified and saved must be applied to devices with the same vendor and release.

Access to the script management is controlled by the administration, script management and script execution scope of command roles. Access to auto-provision is controlled by the auto config permissions that are defined in the scope of command roles. Users that are assigned the administration or script management role can create, modify, delete, and execute scripts. Users that are assigned the script execution role can view and run scripts, view and save results, configure script targets and sources, and view historical results.

In addition to the scope of command access roles and profiles, access to the Scripts tool is further defined by span of control. Span of control profiles determine where a user can apply scope of command access roles and profiles. For example, a user may have privileges to execute scripts. However, a span of control profile defines the scripts that the user can execute.

Auto-provision requires a Mobile Services Package license key to operate. See chapter 3 for more information about obtaining and installing software license keys.

21.2 Workflow to configure network devices using auto-provision

1 Configure the source template. See Procedure 21-1 for more information.

   i Determine the NE configuration that you need to use for the source.

   ii Import a source configuration file from the router, or create a source file by performing a backup of the source configuration and naming the backup file a unique name.

   iii Generate a template from the source script.

2 Configure the target template. See Procedure 21-2 for more information.

   i Import the template file to the auto-provision profiles tool.

   ii As required, configure the source script.

   iii Use the GUI builder to customize attributes in the source template. Refer to the *5620 SAM Scripts and Templates Developer Guide* for more information.

3 Apply a target template to an unprovisioned NE. See Procedure 21-3 for more information



Note — Typically, step 1 is performed on one 5620 SAM, and steps 2 and 3 are performed on another 5620 SAM. Step 1 is typically performed in a lab or testing environment.

21.3 Auto-provision procedures

Use the following procedures to perform auto-provision.

Procedure 21-1 To configure a source template

1 Choose Tools→Auto-Provision Profiles from the 5620 SAM main menu. The Auto-Provision Profiles form opens.

2 Choose Auto-Config Source Node Profile (Automatic Configuration) from the drop-down menu.

3 Click on the Create button. The Auto-Config Source Node Profile (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Auto-Assign ID
- Script ID
- Name
- Description
- Network Element Type
- Network Element Version Information

5 Click on the Select button beside the Source Node Name parameter. The Select Source Node Auto-Config Source Node Profile form opens.

6 Choose a source NE from the list and click on the OK button. The Select Source Node Auto-Config Source Node Profile form closes. The following source NE information is displayed:

- Name
- Management IP Address
- System ID (Loopback IP Address)
- Chassis Type
- Software Version

7 Click on the Apply button. The Backup State parameter displays the status of the last backup operation on the NE, and the Script tab is available.

8 Create a backup file of the source NE and import the configuration script by performing one of the following:

a Back up and import from the router.

i Click on the Backup button. If the Backup button is not visible, click on the More Actions button and choose Backup. The Backup State parameter displays the status of the backup. When the status is Success, go to step ii.

ii Click on the Attach Source Node Config button. If the Attach Source Node Config button is not visible, click on the More Actions button and choose Attach Source Node Config. The backed-up script is attached to the source profile and can be viewed from the Script tab.

b Back up and import the device configuration to a file.

i See “To export a device backup to a file” in the *5620 SAM System Administrator Guide* for information about saving a 7705 SAR configuration to a backup file.

ii Click on the Script tab and click on the Create button. A Script Editor window opens.

iii Choose File→Import from the Editor menu. The Import dialog box appears.

iv Scroll to the location of the backup file that you previously created and saved.

v Click on the Import button. The script appears in the Script Editor workspace.

vi Choose File→Save and Close from the Editor menu. The Script Editor form closes.



Warning 1 — Scripts that are not correctly applied or created can cause serious damage to the network. Alcatel-Lucent recommends that system administrators clearly define the user responsibilities for script usage, and ensure that scripts are verified before they are executed on devices in a live network.

Warning 2 — Before you run a script, you need read, write, and execute permissions for the following directories:

- *install_dir*/client/nms/bin, on a RHEL or Solaris station
- *install_dir*\client\nms\bin\clientCache, on a Windows station

where *install_directory* is the 5620 SAM client installation location, typically /opt/5620sam/client on RHEL and Solaris, and C:\5620sam\client on Windows.

vii Choose File→Save and Close from the Editor menu. The Script Editor form closes and the Auto-Config Source Node Profile (Edit) form reappears. The script appears in the list.

9 Click on the Generate Template button. If the Generate Template button is not visible, click on the More Actions button and choose Generate Template.

Template generation can take several minutes to complete depending on the size of the source configuration file and server resource usage. After the process is complete, the Template tab is available.

10 Click on the Template tab. The newly created template appears in the list.

11 Choose a template and click on the Properties button. The script appears in the Script Editor workspace.

12 See "Velocity GUI builder" in the *5620 SAM Scripts and Templates Developer Guide* for more information about using the GUI builder tool to generate and customize a UI.

13 Choose File→Save from the Editor menu and close the GUI Builder window. The Script Editor window reappears.

14 Choose File→Export from the Editor menu. The Export dialog box appears.

15 Scroll to the location where you need to save the text file and enter a file name.

16 Click on the Export button. The Script Editor window reappears.

17 Close the Script Editor window. A dialog box appears if you entered any changes to the script.

18 Click on the OK button to save the changes to the script.

19 Close the Auto-Config Source Node Profile (Edit) form.

Procedure 21-2 To configure a target template

1 Choose Tools→Auto-Provision Profiles from the 5620 SAM main menu. The Auto-Provision Profiles form opens.



Note — Before you can apply a source configuration to a target NE, you must configure and export the source configuration. See Procedure 21-1 for more information about configuring and exporting a source template.

2 Choose Auto-Config Target Node Profile (Automatic Configuration) from the drop-down menu.

3 Click on the Create button. The Auto-Config Target Node Profile (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Auto-Assign ID
- Script ID
- Name
- Description
- Network Element Type
- Network Element Version Information

5 Click on the Apply button. The Template and Targeted Nodes tabs are available.

6 Click on the Template tab and click on the Add button. A Script Editor window opens.

7 Choose File→Import from the Editor menu. The Import dialog box appears.

8 Scroll to the location of the file that you exported in Procedure 21-1.

9 Click on the Import button. The script appears in the Script Editor workspace.

10 See "Velocity GUI builder" in the *5620 SAM Scripts and Templates Developer Guide* for more information about using the GUI builder tool to generate and customize a UI.

11 Choose File→Save from the Editor menu and close the GUI builder window.

12 Choose File→Save and Close from the Editor menu. The Script Editor form closes and the Auto-Config Target Node Profile (Edit) form reappears displaying the template.

13 Close the Auto-Provision Target Node Profile (Edit) form. To apply the source template to a target NE; go to Procedure 21-3.

Procedure 21-3 To apply a target template to an unprovisioned NE

1 Choose Equipment from the drop-down menu on the navigation tree.



Note — You can also access the Auto-Provision Managed Node Wizard from the equipment properties configuration form.

2 Right-click on the target device in the navigation tree and choose Auto-Provision from the drop-down menu. The Auto-Provision Managed Node Wizard form appears with the Profile step displayed.



Note — When a device has been previously configured, the Auto-Provision option is dimmed for the device.

3 Click on the Select button beside the Script ID parameter. A Select Template Name (Profile) - Auto-Provisioning form opens displaying a list of templates.

4 Choose the target template that you configured in Procedure 21-2.

5 Click on the OK button. The Auto-Provision Managed Node Wizard reappears.

6 Perform one of the following:

- **a** Enable the Adjacent NE Managed parameter when the adjacent NE is managed by the 5620 SAM. Go to step 9.
- **b** Disable the Adjacent NE Managed parameter when the adjacent NE is not managed by the 5620 SAM.

7 Click on the Next button. The Adjacent Node step is displayed.

8 Configure the Adjacent Site ID parameter. Go to step 13.

9 Click on the Next button. The Adjacent 7750 Node step is displayed.

10 Click on the Select button beside the Name parameter. A Select Adjacent NE - Auto-Provision Site form opens with a list of NEs.

11 Choose an NE from the list.

12 Click on the OK button. The Auto-Provision Managed Node Wizard reappears with the information about the displayed NE.

13 Click on the Finish button. A dialog box appears prompting you to deploy the script and generate configuration modules for the adjacent device.

14 Click on the OK button. The 5620 SAM prompts you to view the newly created auto-provision configuration.

15 Enable the View the newly created Auto-Provisioning parameter to display the auto-provision configuration after you close the form, if required.

16 Click on the Close button. The Auto-Provision-Site (Edit) form opens displaying the provisioning for the adjacent device.

17 Click on the Deploy Profile button. A Target Configuration form opens displaying the target NE, and the configurable parameters.

18 Configure the parameters, as required.

19 Click on the NE to which you need to deploy the configuration profile.

20 Click on the Execute button. View the status of the auto-provisioning in the Detailed Status/Error panel. After the NE is configured using the configuration profile, the status of the NE changes to configured.

21 Click on the Modules tab.



Note — You must deploy the 7750 SR configuration modules after the 7705 SAR auto-provisioning is successfully deployed and resynchronized.

22 Click on the Generate Modules button to prompt the 5620 SAM to display the interactions between the target device and the adjacent device.

23 Click on the Properties button of a generated module to configure all of the modules that were created. The default values for some of the modules are usable. However, for other modules such as SAP modules, the operator must select a port on the 7750 SR before performing step 24.

24 Click on the Deploy Modules button to configure the connection.

25 Click on the Service Associations tab to view the modified services.

26 Close the Target Configuration form.

Network management

22 — NE routing and forwarding

23 — Protocol configuration

24 — NAT

25 — MPLS

26 — MPLS-TP

27 — Service tunnels

28 — Lawful Intercept

29 — IPsec

30 — ISA-Video

31 — Alarm management

32 — OAM diagnostic tests

33 — VRRP

34 — APS

35 — lightRadio Wi-Fi

36 — MC peer groups

37 — MC IPsec

38 — MC endpoint groups

39 — MC LAG groups

40 — MC synchronization groups

41 — MC ring groups

22 — NE routing and forwarding

22.1 NE routing and forwarding overview *22-2*

22.2 Network domain overview *22-12*

22.3 Workflow to configure NE routing and forwarding *22-12*

22.4 Workflow to configure network domains *22-14*

22.5 NE routing and forwarding configuration procedures *22-15*

22.6 Network domain configuration procedures *22-78*

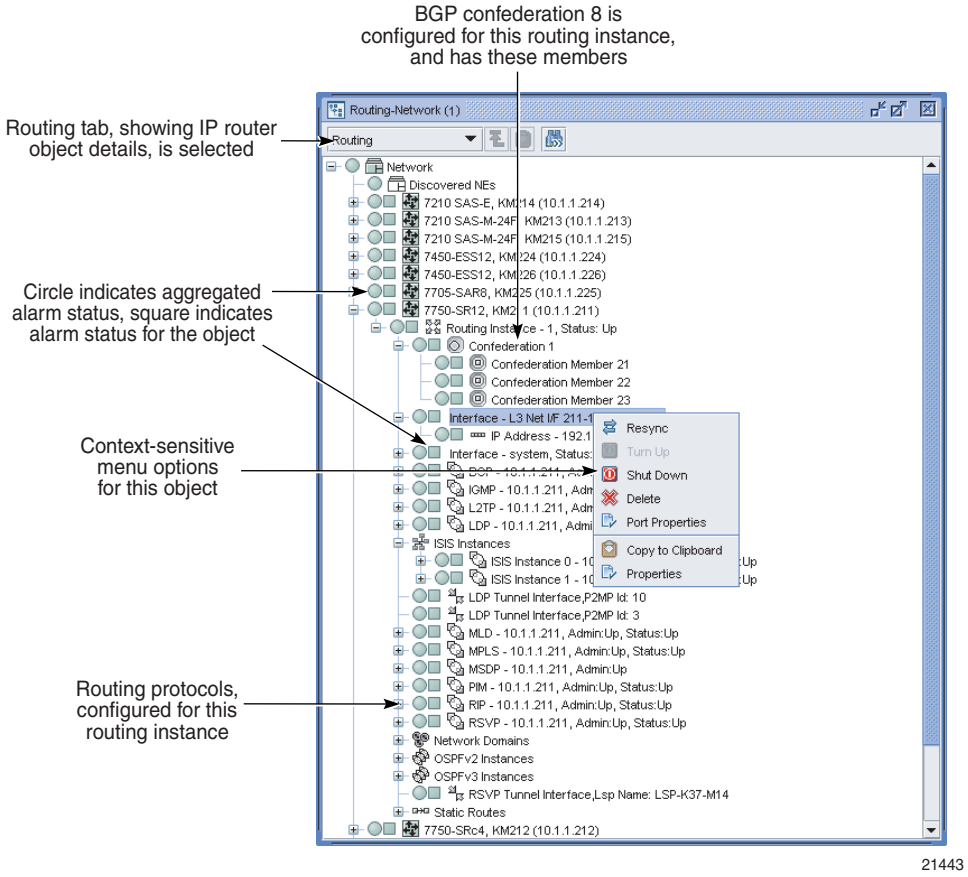
22.1 NE routing and forwarding overview

The 5620 SAM allows you to view and configure the routing and forwarding parameters on NEs. You can use the Routing view in the 5620 SAM GUI navigation tree to manage these functions on each managed NE.

Note — For an OmniSwitch, the 5620 SAM supports viewing the status of routing protocols that are enabled using the CLI. The 5620 SAM also supports the configuration and management of routing instances, L3 interfaces, and static routes.

Figure 22-1 shows the routing objects in the network view of the navigation tree.

Figure 22-1 Routing objects



L3 network interfaces

An L3 network interface is a logical IP object that is defined on a physical port, such as an Ethernet port. An L3 interface:

- associates an IP address and subnet mask with a physical port or channel
- has a physical port or channel cabled to another device

- requires QoS policy configuration
- requires routing protocol configuration

The physical connection of one device to another device is through a port or channel. However, the L3 interface determines its IP connectivity. The L3 interface passes both routing information and IP traffic.

The system interface is associated with a network entity, such as a specific device, not a specific interface. The system interface is also referred to as the loopback interface. The system interface is associated during the configuration of the following entities:

- the termination point of service tunnels
- the hops when configuring MPLS paths and LSPs
- the addresses on a target device for BGP and LDP peering

The system interface is used to preserve connectivity when an interface fails or is removed. A system interface must have an IP address and a 32-bit subnet mask. The system interface is used as the device identifier by higher-level protocols such as OSPF and BGP. See chapter 23 for more information about routing protocols.

DoS protection

In a subscriber aggregation network, an NE typically receives few control-plane packets from a specific subscriber. If one or more subscribers generate excessive control-plane traffic, DoS protection policies can help to ensure that NEs do not become overburdened by these unwanted packets. Global DoS protection controls the arrival rate for unprovisioned link-layer protocol packets from CE devices.

You can use the 5620 SAM to create DoS protection policies and apply them to L3 network interfaces. A DoS protection policy limits the number of control-plane protocol packets that are received each second from a subscriber host, and optionally logs a violation notification if a policy limit is exceeded. The interface drops the excessive packets before they are queued or processed by the NE. You can use the NE System Security form to view the violations for a specific NE.

You can apply DoS protection policies to control the following on L3 network interfaces:

- the control-plane packet arrival rate per subscriber host
- the overall control-plane packet arrival rate for the interface
- whether an NE sends a notification trap if a policy limit is exceeded

An NE that supports DoS protection automatically assigns a default DoS protection policy to each L3 network interface. The default policy limits only the overall packet arrival rate for the interface, and cannot be deleted or modified.

You can also apply DoS protection policies to certain L2 and L3 access interfaces. See the appropriate service chapter for information about applying DoS protection policies to access interfaces.

You can configure a global NE DoS protection policy and distribute it to NEs by choosing Administration→Security→NE DoS Protection from the 5620 SAM main menu. See "To configure an NE DoS protection policy" in the *5620 SAM System Administrator Guide* for more information about configuring and applying NE DoS protection policies.

DDoS protection

You can configure a global NE DDoS protection policy and distribute it to NEs by choosing Administration→Security→NE DDoS Protection from the 5620 SAM main menu. You can configure a DDoS protection policy on an L3 network interface. See "To configure an NE DDoS protection policy" in the *5620 SAM System Administrator Guide* for information about configuring a DDoS protection policy.

Routing protocols

When you configure a device, you configure the routing protocols used and the topology of packet handling between different devices in the network.

Networks can be grouped into areas. An area is a collection of network segments within an AS that have been administratively assigned to the same group. Area topology is concealed from the rest of the AS. This means a significant reduction in routing traffic. Routing in the AS takes place on two levels, depending on whether the source and destination of a packet reside in:

- the same area, known as intra-area routing
- different areas, knows as inter-area routing

In intra-area routing, the packet is routed based on information found within the area; no routing information from outside the area is used. This protects intra-area routing from the injection of bad routing information. Two devices, which are not area border routers, and belonging to the same area, have identical topological databases.

Devices that are aware of more than one area are called area border routers. In this case, all devices in an AS do not have an identical topological database. An area border router has a separate topological database for each area it is connected to. ASs share routing information, such as routes to each destination and information about the route or AS path, with other ASs using BGP.

Routing tables contain lists of next hops, reachable addresses, and associated path cost metrics to each device. Routing protocols use the information and path parameters to compile a network topology. The information about routes that is used to update routing tables can be modified using routing policies.

Fast Re-route

Fast Re-route (FRR) allows the user to provide local protection for an LDP FEC by pre-computing and downloading to the IOM both primary and backup next hops for the FEC.

FRR provides for the use of the Loop-free Alternate (LFA) backup next-hop for forwarding in-transit and CPM generated IP packets when the primary next-hop is not available. IP FRR is supported on IPv4 and IPv6 prefixes forwarded in the base router instance over a network IP interface, or an IES SAP or spoke interface. It is also supported for VPRN VPN-IPv4 prefixes and VPN-IPv6 prefixes forwarded to a VPRN SAP or spoke interface.

FRR requires SPF computation of an LFA next-hop (in addition to the primary next-hop) for all prefixes used by LDP to resolve FECs. The LFA next-hop is populated into the routing table along with the primary next-hop for each prefix.

LFA is configured on IS-IS routing instances, enabling LFA computation by SPF under the IS-IS routing protocol. The LFA next hop can be excluded individually on the IS-IS Level 1 and IS-IS Level 2 objects, as well as on IS-IS interface objects.

LFA is configured on OSPF routing instances, enabling LFA computation by SPF under the OSPF routing protocol. The LFA next hop can be excluded individually on the OSPF area objects, as well as on OSPF interface objects.

LLDP

Link Layer Discovery Protocol is a not a routing protocol, but instead, a neighbor-discovery protocol. As such, it is configured in a different manner than the standard routing protocols. LLDP allows a network access device to advertise its identity and capabilities to other stations attached to the same physical IEEE 801 LAN. It also permits information that the devices discover about peer devices to be stored. LLDP is only applicable for devices using Ethernet connectivity.

When LLDP is enabled on a device, it sends and receives LLDP messages on all of the physical interfaces that are enabled for LLDP transmission. These messages are sent periodically to ensure that information is accurate. These messages are stored on the local device for a configurable amount of time, and after this time has expired, the information is discarded.

5620 SAM uses the information stored in the applicable LLDP tables on the node to automatically discover the physical topology in the network. You can use this information to examine the L1/L2 topology and perform appropriate diagnostics and troubleshooting.

In LLDP, a single LLDP Protocol Data Unit is transmitted in a single Ethernet frame. The basic LLDP PDU consists of a header, followed by a variable number of information elements known as TLVs that each include fields for Type, Length, and Value. Type identifies what kind of information is being sent. Length indicates the length of the information string. Value is the actual information sent. Each LLDP PDU includes three mandatory TLVs followed by optional TLVs.

Mandatory TLVs include:

- Chassis ID: this represent the chassis identification of the device transmitting the LLDP frame
- Port ID: this represents the identification of the specific port transmitting the LLDP frame
- TTL: this represents the length of time the receive frame shall be valid

Optional TLVs include:

- Port Description: this represents the description of the port
- System Name: this is the administratively-assigned name of the device
- System Description: this is a textual description of the device
- System Capabilities: this identifies the capabilities of the device and its function (such as router, switch, repeater, etc.)

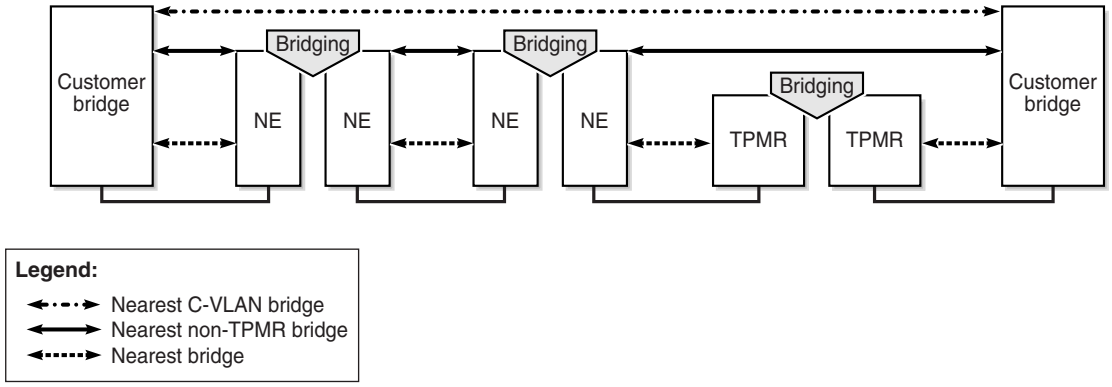
LLDP also supports multiple transmission scopes. The destination MAC address in the LLDP PDU determines how a frame is propagated through the network, thereby determining the LLDP message scope. Table 22-1 identifies a set of destination MAC address and describes the different transmission scopes associated with each address.

Table 22-1 MAC Addresses and transmission scopes

Name	Value	Purpose
Nearest Bridge	01-80-C2-00-00-0E	Propagation constrained to a single physical link
Nearest non-TPMR bridge	01-80-C2-00-00-03	Propagation constrained by all bridges other than TPMR; intended for use within provider bridged networks
Nearest Customer Bridge	01-80-C2-00-00-00	Propagation constrained by customer bridges

This information is also presented graphically in Figure 22-2.

Figure 22-2 LLDP Multiple Transmission Scopes



To enable LLDP, you must configure the protocol at both the system level and at the port level. This is best done using the equipment navigation tree. Table 22-2 lists the procedures required to implement LLDP.

Table 22-2 LLDP configuration procedures list

Procedure	See
To enable LLDP on a router	Procedure 13-12
To configure Ethernet ports	Procedure 16-1
To configure OmniSwitch Ethernet ports	Procedure 16-23

You can also use the physical topology map to view and edit various LLDP parameters and interconnections. By default, the physical map displays the topology based on the nearest-bridge LLDP scope. In addition, after the physical topology of a network has been discovered, you can create a reference checkpoint which is basically a snapshot of the topology at a specific time. Any subsequent deviations from this checkpoint can then be displayed. See "Physical topology map" in section 6.1 for more information.

Routing policies

Routing policies, also known as route redistribution policies, control the size and content of the routing tables, the routes that are advertised, and the best route to take to reach a destination.

The 5620 SAM supports routing-policy distribution to the following devices:

- 7210 SAS-M24F
- 7210 SAS-M24F2XFP
- 7210 SAS-M24F2XFP [ETR]
- 7210 SAS-X24F2XFP
- 7950 XRS
- 7450 ESS
- 7705 SAR
- 7710 SR
- 7750 SR

There are no default routing policies. Each policy must be created and applied to an object, a routing protocol, or the forwarding table. Each set of rules that is associated with controlling routes are called routing policy statement entries on the client GUI.

Use routing policies:

- to control routing protocols, such as BGP, to allow routes from another protocol, such as OSPF, into the routing table, which allows the routing table to redistribute packets into other protocols
- to control the import and export of learned active routes of a protocol
- to modify the characteristics of a route, for example, to change the community values of BGP AS path attributes
- to prevent the routes for specific customers from being added to routing tables
- to control BGP route flapping

Routing policy statements and routing policy statement entries are compared against incoming route packets in the following sequence.

1 The routing packets arrive.

2 The first routing policy is analyzed.

3 Each entry in the routing policy statement is analyzed.

If a match is found based on the first routing policy statement entry, the specified action is performed. You can use the Action parameter to specify the continued evaluation of route policy entries, or additional policy statements.

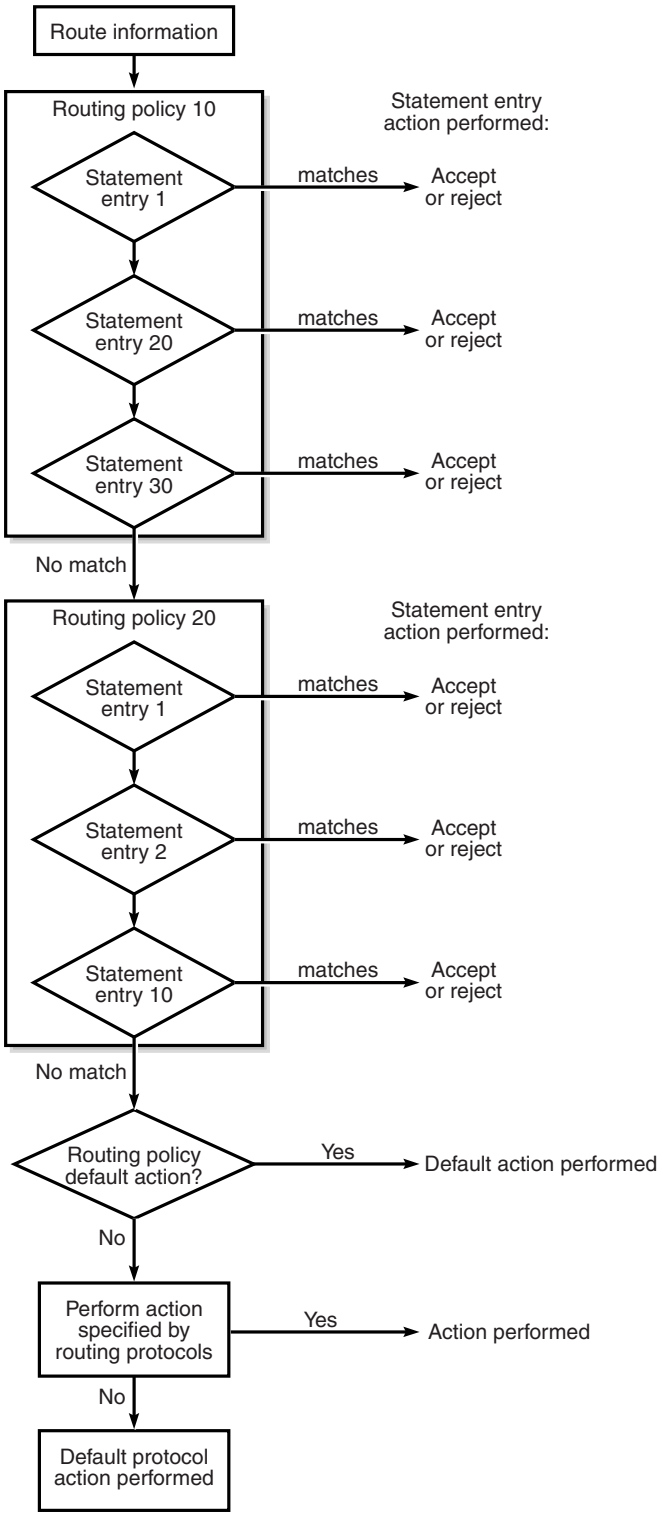
4 If no match is found, the packet is compared against the second routing policy statement entry. If a match is found based on the second routing policy statement entry, the specified action is performed.

5 If no match is found, the packet is compared sequentially against all remaining routing policy statements and routing policy statement entries. If a match is found, the specified action is performed.

6 If the packet does not match any routing policy statements or entries, the default action is performed.

Figure 22-3 shows how routes are analyzed using routing policies.

Figure 22-3 Routing policy analysis workflow



To ensure routing configuration flexibility, the following routing policies can be configured as separate policies or can be cross-referenced to form a framework of policies depending on the network requirements:

- Policy Statement
- Prefix List
- Community
- Damping
- AS Path

Policies that are cross-referenced are distributed together. For example a Policy Statement can reference the Prefix List policy by matching the From Criteria and the To Criteria for each policy type.

Careful planning is essential to implement route policies that can affect the flow of routing information or packets traversing managed devices. Before configuring and applying a route policy, consider the following:

- Develop an overall plan and strategy to accomplish your intended routing actions
- Analyze the effect of what happens to a packet that meets the specified criteria in a routing policy statement entry to ensure the proper action is executed and that no routing loops are created
- when possible, redistribute from a less router protocol to a greater routing protocol, for example from RIP to OSPF
- redistribute exported routes at a single device, when possible

When no action or default action in a routing policy is matched on a packet, then the routing protocols determine the default action for the packet. The action can be specified for the protocol. If the action is not specified, there are default routing protocol import and export actions performed, as described in Table 22-3.

Table 22-3 Default routing protocol actions

Protocol	Default import route action	Default export route options
BGP	All routes from BGP peers are accepted and forwarded to the BGP route selection process.	All active internal BGP routes are advertised to BGP peers. All non-BGP learned routes are not advertised to BGP peers.
IS-IS	IS-IS route acceptance cannot be configured. All IS-IS routes are accepted from IS-IS neighbors.	All internal IS-IS routes are advertised to all IS-IS neighbors. All non-IS-IS learned routes are not advertised to IS-IS neighbors.
OSPF	OSPF route acceptance cannot be configured. All OSPF routes are accepted from OSPF neighbors.	All OSPF routes are advertised to all OSPF neighbors. All non-OSPF learned routes are not advertised to OSPF neighbors.
RIP	All RIP-learned routes are accepted from RIP peers.	All non-RIP learned routes are not advertised to RIP peers.

For importing routing, RIP, BGP, or OSPF learned routes can be altered using routing protocols. For example, for devices learning about routes from BGP or OSPF, you can create an import route policy that can limit the number and types of routes accepted and added to the routing tables.

For exporting routes, some default behaviors exist:

- internally learned routes are redistributed using the same protocol
- externally learned routes are not automatically advertised to all neighbors or peers

In the case of externally learned routes, you can create an export policy to determine how the routes are advertised, for example, configuring something learned by BGP to be redistributed using OSPF. This is useful in cases:

- where legacy equipment does not support a specific protocol
- when companies merge and they use different routing protocols on the devices

Cflowd

Cflowd collects statistical data based on traffic flows. A flow is a series of packets in a user session. Cflowd data is typically used to monitor network usage trends and detect security threats. You can use the 5620 SAM to configure Cflowd for:

- traffic that passes through an L3 network interface
- traffic that is redirected to cflowd using an ACL IP filter
- AA traffic

The 5620 SAM supports the configuration of cflowd on the following NE types, depending on the release and chassis type: 7450 ESS, 7710 SR, 7750 MG, 7750 SR, and 7950 XRS.

You must enable cflowd globally on an NE before you can configure cflowd collectors. You can create multiple cflowd collectors on an NE. Each collector is deleted if cflowd is disabled.

AA cflowd is configurable on an ISA-AA group, and supports basic cflowd sampling as well as TCP performance data collection for AA applications and application groups. Each ISA-AA group supports one cflowd instance.

See chapter 13 for information about enabling and configuring global cflowd on an NE, and see chapter 14 for information about enabling and configuring AA cflowd on an ISA-AA group.

Shared Risk Link Group policies

Shared Risk Link Groups, or SRLGs, are constructs which allow you to perform two operations that enhance overall system reliability. You can use SRLGs to establish a FRR LSP path. You can also use SRLGs to establish a secondary LSP path which is disjointed from the primary LSP path. Links that are members of the same SRLG represent resources which share the same risk. For example, fiber links sharing the same conduit, or multiple wavelengths sharing the same fiber.

An SRLG is modeled as a policy object. It therefore follows the normal policy behavior for creation, listing, updating, deletion, distribution, and re synchronization.

Configured SRLGs are associated with MPLS interfaces. The SRLGs are used by the CSPF when computing a FRR detour/bypass path, or a secondary LSP path. SRLGs indicate to the CSPF which interfaces to avoid in the path's computation.

22.2 Network domain overview

The 5620 SAM allows you to create, delete, associate and edit network domains. You can use the network domains view in the 5620 SAM GUI navigation tree to manage these functions. Network domains help determine which network ports are eligible to transport traffic of individual SDPs. This information is used for the SAP-ingress queue allocation which is applied to VPLS SAPs. No SAP-ingress queues are allocated if a given port does not belong to the network domain used in a VPLS.



Note 1 — A maximum of four network domains are supported in any VPLS.

Note 2 — If an SDP is used for E-PIPE, I-PIPE or A-PIPE bindings, the network domain configuration is not considered.

Note 3 — Network domains are not applicable to loopback and system interfaces.

By default, all network interfaces in a routing instance belong to the default network domain. You can associate an interface to any user defined network domain. The loopback and system interfaces cannot be associated with user defined network domains.

An SDP can be assigned to only one network domain. If no user defined network domain is created, an SDP will be assigned to the default network domain. All SAPs in VPLS will have a queue reaching all fwd complexes serving interfaces belonging to the same network domains as the SDPs. You can assign or remove a network domain association of the interface or SDP without deleting the respective object.

22.3 Workflow to configure NE routing and forwarding

1 Use the CLI to configure or verify the following parameters:

- system address (system ID)
- router ID

See the *7750 SR OS Router Guide* for more information about these parameters.

2 Configure a routing instance or VRF instance:

a To configure a routing instance or VRF instance, see Procedure 22-1.

b To configure a local DHCPv4 server on the routing instance, see Procedure 22-2. To configure a local DHCPv6 server on the routing instance, see Procedure 22-3.

c To configure a routing instance on the OmniSwitch, perform the following:

i Configure a routing instance on the OmniSwitch. See Procedure 22-5.

ii Configure UDP relay/DHCP snooping on an OmniSwitch, if required. See Procedure 22-6.

iii If you configured UDP relay/DHCP snooping, then configure all ports within the network connected to DHCP servers to trusted. See Procedure 16-23.

d To configure NAT on the routing instance, see Procedure 24-3 in chapter 24.

e To configure RADIUS servers on the routing instance, see Procedure 22-7.

f To configure RADIUS proxy servers on the routing instance, see Procedure 22-8.

3 Create or configure network or system L3 interfaces.

a On all NEs except the OmniSwitch. See Procedures 22-9 and 22-10.

i Associate a network port with the L3 interface.

ii Configure the appropriate routing protocols on the interfaces, as required. The supported protocols are BGP, MPLS, RIP, LDP, OSPFv2, OSPFv3, IS-IS, and RSVP. See chapter 23 for more information about routing protocol configuration and parameters.

iii Enable the multicast routing types on the interfaces as required. The supported types are PIM, IGMP, and MLD. See chapter 23 for more information about multicast configuration and parameters.

iv Enable bridging on the interfaces as required. The 5620 SAM supports bridging on OmniSwitch devices. See chapter 23 for more information about bridging configuration and parameters.

v Assign a DoS protection policy to the interface, if required. See procedure 22-10 for more information.

vi Assign an IES or network interface to a virtual router as a VRRP instance. See chapter 33 for more information about VRRP configuration and parameters.

b On an OmniSwitch. See Procedures 22-11 and 22-12 for more information.

4 Create static routes, as required. See Procedure 22-13 for all NEs except the OmniSwitch. See Procedure 22-14 for the OmniSwitch.

5 Cable the network ports on the devices to the network ports on other devices.

6 Configure these key device parameters using the 5620 SAM:

- BGP, MPLS, RIP, LDP, OSPF, IS-IS, and RSVP
  Enable routing protocols on the device, as required. If you plan to create signaled LSPs, then you must enable MPLS, and RSVP or LDP.
- IP address ranges for use by services, such as IES and VPLS
  Reserve IP addresses to provide a mechanism to reserve one or more address ranges for services. When services are defined, the address must be in the range specified as a service prefix. Addresses in the range of a service prefix can be allocated to a network port unless set to exclusive. Then, the address range is exclusively reserved for services.
- device-wide AS settings

7 Configure the appropriate routing policies as required:

i Routing policy statements. See Procedure 22-15.

ii Prefix list policy. See Procedure 22-16.

iii Community policy. See Procedure 22-17.

iv Damping policy. See Procedure 22-18.

v AS path policy. See Procedure 22-19. If required, configure BGP for the AS path policy. Configuring BGP optional and should only be implemented to reduce the IBGP mesh inside an AS. An AS can be logically divided into smaller groupings called sub-confederations. See chapter 23 for more information about BGP configuration.

vi MPLS administrative group policy. See Procedure 22-21.

vii Shared Risk Link Group policy. See Procedure 22-22. If required, create a static configuration for the SRLG Policy, see Procedure 22-23.

8 View the following NE routing and forwarding related objects, as required:

a Current network resources such as IP addresses, duplicate IP addresses, RDs and RTs, and MAC addresses. See Procedure 22-24.

b Routing or VRF instances or related objects. See Procedure 22-25.

c DHCPv6 leases. See Procedure 22-27.

d DHCPv6 log events. See Procedure 22-28.

e Routing policies from a CLI session. See Procedure 22-29.

22.4 Workflow to configure network domains

1 Create a network domain. See Procedure 22-33.

2 Associate a network interface with a network domain. See Procedure 22-34. See Procedure 22-35 to remove a network interface from a network domain.

3 Associate a service tunnel with a network domain. see Procedure 22-36. See Procedure 22-37 to remove a service tunnel with a network domain.

4 Delete a network domain, as required. See Procedure 22-38.

22.5 NE routing and forwarding configuration procedures

The following procedures describe how to configure routing.

Procedure 22-1 To configure a routing instance or a VRF instance

1 Choose Routing from the navigation tree view selector.

2 Navigate to a routing instance icon by choosing Network→NE→Routing Instance.

3 Perform one of the following:

a If you are configuring a VRF routing instance on the following OmniSwitch NEs, go to step 4.

- OS 6850E
- OS6855-U24X
- OS 6900
- OS 9700E
- OS 9800E
- OS 10K

b If you are configuring a routing instance, go to step 6.

4 Right-click on the OmniSwitch routing instance icon and choose Create VRF Instance from the menu. The Routing Instance (Create) form opens.

5 Configure the VRF Name parameter. Click on the Apply button. The Routing Instance (Edit) form opens. Go to step 9.

6 Right-click on the routing instance icon and choose Properties from the menu. The Routing Instance (Edit) form opens with the General tab displayed.

7 Configure the Administrative State parameter.

8 If you are configuring a routing instance on a 7750 SR, click on the Select button next to the Reassembly Group field and choose an ISA-BB group from the Select ISA-BB Group form. Only ISA-NAT and ISA-WLAN GW groups are selectable. Otherwise, go to step 9.

9 Click on the Protocols tab.

10 Configure the applicable parameters:

- BGP Enabled
- MPLS Enabled
- OSPFv2 Enabled
- RIP Enabled
- L2TP Enabled
- LDP Enabled
- MPLS-TP Enabled
- RSVP Enabled
- OSPFv3 Enabled
- IS-IS Enabled
- WPP Enabled

The supported protocols are displayed in the navigation tree as sub-items in the routing instance. Click on the Properties button to configure the routing protocols. See chapter 23 for more information about routing protocol configuration using the GUI.



Note — SNMPv3 must be used to manage supported OmniSwitch devices when configuring a VRF routing instance.

11 Click on the Edit Routing Policies button. If the Edit Routing Policies button is not visible, click on the More Actions button and choose Edit Routing Policies. The Routing Policy Manager (Edit) form opens with the General tab displayed.

12 Click on the Show Policy button. If the Show Policy button is not visible, click on the More Actions button and choose Show Policy. A Routing Policy Show Policy form opens. A CLI display is initiated.

13 View the policy.

14 Click on the Close button. The Routing Policy Show Policy form closes.

15 Close the Routing Policy Manager (Edit) form.

16 Click on the Multicast tab.

17 Configure the parameters:

- PIM Enabled
- IGMP Enabled
- MLD Enabled
- MSDP Enabled

The supported multicast protocols are displayed in the navigation tree as sub-items in the routing instance. Click on the Properties button to configure the routing protocols. See chapter 23 for more information about how to configure multicast protocols.

18 Click on the Routing tab.

19 Configure the parameters:

- Router ID
- Maximum Number of Equal Cost Routes
- Autonomous System
- Confederation Autonomous System
- LDP Shortcut Enabled
- Enforce Maximum Number Of Multicast Routes
- Fast Re-route

For the 7210 SAS-M and 7210 SAS-X, the value for the Maximum Number of Equal Cost Routes parameter cannot be greater than the value of the Max ECMP Route Destinations (Active) parameter in the system resource profile. See Procedure 13-20.

The Fast Re-route parameter is configurable only on the 7950 XRS, and on the 7750 SR and 7710 SR in chassis administrative mode D.

When you select the Enforce Maximum Number Of Multicast Routes parameter, the following configurable parameters appear:

- Maximum Number Of Multicast Routes
- Log Only
- Threshold (%)

See chapter 23 for more information about AS and confederation parameters for BGP using the GUI.

20 Configure the parameters:

- Single SFM Overload Admin State
- Hold-Off Time (seconds)

The Hold-Off Time (seconds) parameter and read-only attributes Overload State, Overload Start, and Overload Duration are only displayed when the Single SFM Overload Admin State parameter is set to Up.

21 Configure a Multicast Path Management Info Policy, if required.

i Click on the Select button beside the Name parameter. The Select Ingress Info Policy form is displayed.

ii Choose the required policy and click OK. The Select Ingress Info Policy form closes and the policy name is displayed in the Name field.



Note — The Mcast Path Mgmt Channels tab displays data on the operational channels after actual traffic from a specific multicast source for a specific multicast group passes through the virtual router. You must click on the Search button to refresh the data. See chapter 42 for a listing of the displayed operational channel parameters.

22 To configure WLAN gateway functionality for the routing instance, do the following:

i Click on the General tab and configure the Enable WLAN GW parameter.

ii Click on the WLAN GW tab.

iii On the General child tab, configure the APN Network Identifier parameter.

iv Click on the Mobile GW Address Map child tab.

v Click on the Create button. The Mobile Gateway Address Map form opens.

vi Configure the Mobile Gateway Address Prefix and Prefix Length parameters.

vii Click on the Select button beside the Mobile Gateway Profile field to specify a mobile gateway profile policy.

viii Repeat steps v through vii to create additional MG address maps.

ix Click on the OK button. The Mobile Gateway Address Map form closes.

23 Click on the Interfaces tab. See Procedure 22-9 for more information about creating additional L3 interfaces.

24 Click on the Address tab.

25 Configure IP address parameters for L3 interfaces.

i Choose an address in the list.

ii Click on the Properties button.

The IP Address form opens.

iii Configure the parameters:

- IP Address
- Prefix Length
- Broadcast Address Format

iv Click on the OK button. The IP Address form closes and the Routing Instance form reappears.



Note — The IP Address, Prefix Length, and Broadcast Address Format cannot be changed for the System interface.

26 Click on the Static Routes tab to view a list of static routes and to add static routes. See Procedure 22-13 for more information.

27 Click on the NAT tab to configure NAT on the routing instance. See Procedure 24-3 in chapter 24 for more information.

28 Click on the RSVP Tunnel Interfaces tab to create an RSVP tunnel interface entry, if required.

i Click on the Create button. The RSVP Tunnel Interface (Create) form opens.

ii Click on the Select button beside the Lsp Name parameter. The Select - RSVP Tunnel Interface form opens.

iii Choose an RSVP tunnel interface and click on the OK button. The Select - RSVP Tunnel Interface form closes and the RSVP Tunnel Interface (Create) form reappears.

iv Configure the Sender Address parameter.

v Click on the OK button. The RSVP Tunnel Interface (Create) form closes.

29 Click on the LDP Tunnel Interfaces tab to create an LDP tunnel interface entry, if required.

i Click on the Create button. The LDP Tunnel Interface (Create) form opens, with the General tab displayed.

ii Configure the parameters:

- Description
- P2MP ID
- Root Node
- Sender Address



Note 1 — When the Root Node parameter is enabled, the LDP tunnel interface you are creating is associated with a root node, and you must specify a unique P2MP ID and Sender Address.

Note 2 — When the Root Node parameter is not enabled, the LDP tunnel interface you are creating is associated with a leaf node, and you must specify the same P2MP ID and Sender Address as the root node.

Note 3 — LDP tunnel interfaces can be created using the system address or any local interface address on the root node.

Note 4 — An LDP tunnel can be created on intermediate nodes (that is, between direct and indirect nodes).

Note 5 — The 7450 ESS only supports LDP tunnel interfaces in Mixed Mode.

iii Click on the Apply button. The LDP Tunnel Interface (Create) form is refreshed.

iv Click on the Tests tab to create a P2MP LSP Ping test, if required.

v Click on the P2MP LSP Ping tab.

vi Click on the Create button. The P2MP LSP Ping form is displayed.

vii Perform Procedure 32-27 to configure and run a P2MP LSP Ping test.



Note — The P2MP LSP Ping test can only be performed on a root node. When this test is created here, the 5620 SAM will auto-populate the Target Type (with the P2MP mLDP option), P2MP ID and Sender Address parameters. If the Root Node parameter is not enabled in step ii above, the Test tab will appear blank.

viii Click on the OK button. The LDP Tunnel Interface (Create) form closes.

30 Click on the Multi-Homing Interface tab to create a multi-homing interface entry, if required. the Multi-Homing Interface (Create) form opens with the General tab displayed.



Note 1 — The Multi-Homing Interface is a loopback interface used in multi-homing resiliency for a pair of protected routers. When it is active, the Primary interface can be used to advertise reachability information of the alternate router to the rest of the network. The Secondary interface is used to resolve routes advertised by the alternate router in the event that router becomes unavailable. This mechanism applies to both IP and VPN traffic.

Note 2 — Only one Primary and one Secondary multi-homing interface can be created for a router.

Note 3 — You can configure a multi-homing interface on the 7950 XRS, 7750 SR, 7710 SR, and 7450 ESS (in mixed mode) network elements. Chassis mode “D” must be enabled.

i Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Type
- Hold Time (seconds)
- Administrative State

The Hold Time (seconds) parameter only appears if you specify Secondary as the Interface Type.

ii Click on the Addresses tab. The Multi-Homing Interface Addresses list is displayed.

iii Click on the Create button. The IP Address (Create) form opens.

iv Configure the IP Address parameter.



Note — Only IPv4 addresses are supported when creating the multi-homing interface.

v Click on the OK button. The IP Address (Create) form closes and the new address appears selected in the list.

vi Click on the OK button. The Multi-Homing Interface (Create) form closes.

31 Click on the Route Aggregation tab to configure route aggregates that can be generated into the virtual router.

i Click on the Create button. The Aggregation (Create) form opens.

ii Configure the parameters, if required:

- IP Address Prefix
- Mask
- Summary Only
- As Set
- Aggregator
- Next Hop Type
- Community
- Aggregator AS
- Aggregator IP Address

The Aggregator AS and Aggregator IP Address parameters are configurable when the Aggregator parameter value is set to True.

The Next Hop Type parameter is configurable only on a Release 10.0 R4 or later 7450 ESS, 7710 SR, or 7750 SR.

The 7705 SAR-8 supports Summary Only route aggregation only.

32 Click on the BGP Confederations tab, if present, to view and create BGP confederations. See chapter 23 for more information about BGP confederation configuration.

33 Resync Soft GRE Tunnels, if required or applicable.

i Click on the Soft GRE Tunnels tab.

ii Click on the Resync Soft GRE Tunnels button.

34 Click on the Service Address Ranges tab, if present, to provide a mechanism to reserve one or more IP address ranges for use by services, such as IES.

i Click on the Create button. The Service Address Range form opens.

ii Configure the parameters:

- IP Address
- Prefix Length
- Exclusive

iii Click on the OK button. The Service Address Range form closes and the Routing Instance form reappears.

35 Configure an override source IP address or L3 interface for use by a selected IP application, if required.

i Click on the Source Address tab.

ii Click on the Create button. The Source Address form opens.

36 Choose an IP application from the Source IP Application drop-down menu.

37 Perform one of the following:



Note — If you choose the interface index option, the router must already have a network interface or an IES L3 access interface created on the routing instance.

a Choose IP Address in Source Address Termination to specify a source IP address on the node for use by the IP application.

i Enter an IP address in the Source IP Address field.

ii Go to step 38.

b Choose Interface Index in Source Address Termination to use the primary address on the L3 network interface as the source address on the node for the IP application.

i Click on the Select button to choose an interface. The Select Source Address Network Interface form opens. Choose an interface in the list and click on the OK button. The IP address and Interface ID of the L3 interface appears on the form.

ii Go to step 38.



Note — You must select an IPv6 Source IP Address to select an IPv6 Source IP Application.

38 Click on the OK button. The Source Address form closes and the Routing Instance form reappears. The IP application source address and parameters appear on the form.

39 Configure a local DHCP server on the routing instance, if required. To configure a local DHCPv4 server on the routing instance, see procedure 22-2. To configure a local DHCPv6 server on the routing instance, see procedure 22-3.

40 Click on the Self Generated Traffic tab. The DSCP Marking tab is displayed with a list of all the applications for which the DSCP can be set.

i Choose an application to view or edit the DSCP setting.

ii Click on the Properties button. An Application DCSP Marking form opens.

iii Configure the DSCP parameter.

iv Click on the OK button. A dialog box appears.

v Click on the Yes button.

41 Click on the DSCP Mapping tab.

i Choose a DSCP mapping in the list and click on the Properties button. The Application DCSP Mapping form opens.

ii Configure the Forwarding Class parameter.

iii Click on the OK button. A dialog box appears.

iv Click on the Yes button.

42 Click on the Dot1p Marking tab.

i Choose a Dot1p marking entry in the list and click on the Properties button. The Application Dot1p Marking form opens.

ii Configure the Dot1p parameter.

iii Click on the OK button. A dialog box appears.

iv Click on the Yes button. The Routing Instance (Edit) form reappears.

43 Close the Routing Instance (Edit) form.

Procedure 22-2 To configure local DHCPv4 server on a routing instance

1 Choose Routing from the navigation tree view selector.

2 Navigate to a routing instance icon by choosing Network→NE→Routing Instance.

3 Right-click on the routing instance icon and choose Properties from the menu. The Routing Instance (Edit) form opens with the General tab displayed.

4 Click on the Local DHCP Servers tab.

5 On the DHCPv4 tab, perform one of the following:

a Create a new DHCPv4 server by clicking on the Create button. The Local DHCP Server (Create) form opens with the General tab displayed.

b Configure an existing DHCPv4 server by choosing an entry and clicking on the Properties button. The Local DHCP Server (Edit) form opens with the General tab displayed.

6 Configure the parameters:

- Server Name
- Description
- Administrative State
- Use Gateway Interface (GI) Address
- Gateway Interface (GI) Address Scope
- Allow Send Force Renews

7 Configure the client pool parameters:

- Use Pool From Client
- Pool Name Delimiter

8 Click on the Select button and choose a local user database from the Local User Db - Local DHCP Server - Site form.

9 Click on the Failover tab to configure DHCP server failover support. The General tab is displayed.

i Configure the Administrative State parameter.

ii Configure the parameters in the Client Lead Time panel:

- Maximum Time (Hours, Minutes, Seconds)
- Ignore Maximum Client Lead Time

iii Configure the Startup Wait Time Minutes and Seconds parameters in the Startup Wait Time panel.

iv Configure the Partner Down Delay Hours, Minutes, and Seconds parameters in the Partner Down Delay panel.

v Click on the Peer tab to configure a failover DHCP server peer.

vi Click on the Create button. The Failover Peer form opens.

vii Click on the Select button and choose a failover peer MCS site from the Select MC Peer form.

viii Configure the Sync Tag parameter. The Synch Tag setting must be the same on both failover servers.

ix Click on the Node Redundancy button to configure node redundancy for the failover peer, if required. The Manage Node Redundancy form opens, preconfigured for MC peer groups.

x Click on the Search button and configure an existing MC peer group, or click on the Create button and configure a new MC peer group. See Procedure 36-1. The Node Redundancy button allows you to access the MC sync group configuration within the MC peer group in order to add failover peer sync tags.

xi Click on OK in the Failover Peer form.

10 Click on the IP Address Pools tab to create a pool of one or more subnets on the local DHCP server.

i Click on the Create button. The IP Address Pool form opens with the General tab displayed.

ii Configure the following parameters:

- Pool Name
- Description

iii Configure the parameters in the Minimum Lease Time panel:

- Days
- Hours
- Minutes
- Seconds

iv Configure the parameters in the Maximum Lease Time panel:

- Days
- Hours
- Minutes
- Seconds

v Configure the parameters in the Offer Time panel:

- Minutes
- Seconds

vi Configure the parameters in the Pool Notifications (Minimum Free) panel:

- Threshold Type
- Threshold Value
- Notify When Pool Is Depleted

vii Configure parameters in the Subnet Binding panel, if required:

- Key
- Unbind Delay (Hours, Minutes, and Seconds)

To specify Unbind Delay values other than the defaults, disable the Default check box.

11 Click on the Subnets tab to add a subnet to the IP address pool.

12 Click on the Create button. The Subnet form opens with the General tab displayed.

i Configure the parameters:

- IP Address
- Prefix Length
- Maximum Declined Addresses Stored
- Subnet Drain
- Threshold Type
- Threshold Value
- Notify When Subnet Is Depleted

ii Click on the Address Ranges tab.

iii Click on the Create button. The Subnet Address Range form opens.

iv Configure the parameters:

- Action
- Start Address
- End Address
- Failover Control



Note — You must exclude static IP addresses from the subnet address range because static IP addresses are dedicated.

v Click on the OK button. The Subnet Address Range form closes and a dialog box appears.

vi Click on the OK button. The Subnet form reappears.

vii Click on the Options tab.

viii Click on the Create button. The Subnet Option form opens.

ix Configure the parameters:

- Option
- Number
- Type
- Value
- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

The Number parameter is configurable when the Option parameter is set to Custom Option.

The Value parameter is configurable when the Type parameter is set to ASCII String or Hex String.

The IP Address 1, IP Address 2, IP Address 3, and IP Address 4 parameters are configurable when the Type parameter is set to IP Address.

x Click on the OK button. The Subnet Option form closes and a dialog box appears.

xi Click on the OK button. The Subnet form reappears.

xii Click on the OK button. The Subnet form closes and a dialog box appears.

xiii Click on the OK button. The IP Address Pool form reappears.

13 Click on the Options tab.

14 Click on the Create button. The IP Address Pool Option form opens.

15 Configure the Option parameter and do one of the following:

a If you set the Option parameter to Custom Option, configure the following parameters:

- Number
- Type
- Value
- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

The Value parameter is configurable when the Type parameter is set to ASCII String or Hex String.

The IP Address 1, IP Address 2, IP Address 3, and IP Address 4 parameters are configurable when the Type parameter is set to IP Address.

b If you set the Option parameter to DNS Name Servers or Netbios Name Server, configure the following parameters:

- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

c If you set the Option parameter to Domain Name, configure the Value parameter.

d If you set the Option parameter to Lease Time, Lease Renew Time, or Lease Rebind Time, configure the following parameters:

- Days
- Hours
- Minutes
- Seconds

e If you set the Option parameter to Netbios Node Type, configure the Netbios Node Type parameter.

16 Click on the OK button. The IP Address Pool Option form closes and a dialog box appears.

17 Click on the OK button. The IP Address Pool form reappears.



Note 1 — The value in the Free Addresses tab specifies the minimum number of free addresses in the pool. If the actual number of free addresses in the pool falls below this configured minimum, an alarm is generated. The value 0 specifies “No minimum”.

Note 2 — The Declined Addresses tab indicates the number of declined addresses.

18 Click on the OK button. The IP Address Pool form closes and a dialog box appears.

19 Click on the OK button. The Local DHCP Server form reappears.

20 Click on the OK button. The Local DHCP Server form closes and a dialog box appears.

21 Click on the OK button. The Routing Instance form reappears.

22 Click on the OK button to save the configuration. A dialog box appears.

23 Click on the Yes button to verify the action.

24 Close the form.

Procedure 22-3 To configure local DHCPv6 server on a routing instance

1 Choose Routing from the navigation tree view selector.

2 Navigate to a routing instance icon by choosing Network→NE→Routing Instance.

3 Right-click on the routing instance icon and choose Properties from the menu. The Routing Instance form opens with the General tab displayed.

4 Click on the Local DHCP Servers tab.

5 Click on the DHCPv6 sub-tab and do one of the following:

a Create a new DHCPv6 server by clicking on the Create button. The Local DHCPv6 Server (Create) form opens.

b Configure an existing DHCPv6 server by choosing an entry and clicking on the Properties button. The Local DHCPv6 Server (Edit) form opens with the General tab displayed.

6 Configure the parameters:

- Server Name
- Description
- Administrative State
- Use Pool From Client
- User Ident
- User Ident
- Use Link Address
- Link Address Scope
- Ignore Rapid Commit
- Interface ID Mapping

7 Configure the parameters in the Lease Hold Time panel:

- Days
- Hours
- Minutes
- Seconds

8 Configure the parameters in the DHCP Unique Identifier panel:

- Server ID Type
- ID Type
- Value



Note — The ID Type and Value parameters are configurable only if the Server ID Type parameter is set to Enterprise.

9 Click on the Failover tab to configure DHCPv6 server failover support.

i Configure the Administrative State parameter.

ii Configure the parameters in the Client Lead Time panel:

- Maximum Time (Hours, Minutes, Seconds)
- Ignore Maximum Client Lead Time

iii Configure the Startup Wait Time Minutes and Seconds parameters in the Startup Wait Time panel.

iv Configure the Partner Down Delay Hours, Minutes, and Seconds parameters in the Partner Down Delay panel.

v Click on the Peer sub-tab to configure a failover DHCPv6 server peer.

vi Click on the Create button. The Failover Peer form opens.

vii Click on the Select button and choose a failover peer MCS server site from the Select MC Peer form.

viii Configure the Sync Tag parameter. The Synch Tag setting should be the same on both failover servers.

ix Click on the Node Redundancy button to configure node redundancy for the failover peer, if required. The Manage Node Redundancy form opens, preconfigured for MC peer groups.

x Click on the Search button and configure an existing MC peer group, or click on the Create button and configure a new MC peer group. See Procedure 36-1. The Node Redundancy button allows you to access the MC sync group configuration within the MC peer group in order to add failover peer sync tags.

xi Click on OK in the Failover Peer form.

10 Click on the IPv6 Address Pools tab to assign one or more pools to the local DHCPv6 server.

11 Click on the Create button. The IPv6 Address Pool form opens with the General tab displayed.

i Configure the following parameters:

- Pool Name
- Description

ii Click on the Prefixes tab to add prefixes to the DHCPv6 server pool.

iii Click on the Create button. The Prefix form opens with the General tab displayed.

iv Configure the following parameters:

- IPv6 Address
- Prefix Length
- Failover Control
- Prefix Type

v Configure the parameters in the Preferred Life Time panel:

- Days
- Hours
- Minutes
- Seconds

vi Configure the parameters in the Valid Life Time panel:

- Days
- Hours
- Minutes
- Seconds

vii Configure the parameters in the Renew Timer panel:

- Days
- Hours
- Minutes
- Seconds

viii Configure the parameters in the Rebind Timer panel:

- Days
- Hours
- Minutes
- Seconds

ix Click on the Apply button. A dialog box appears.

x Click on the OK button.

xi Click on the Options tab.

xii Click on the Create button. The Prefix Option form opens.

xiii Configure the parameters:

- Option
- Number
- Type
- Value
- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

The Number parameter is configurable when the Option parameter is set to Custom Option.

The Value parameter is configurable when the Type parameter is set to ASCII String, Hex String, or Domain.

The IP Address 1, IP Address 2, IP Address 3, and IP Address 4 parameters are configurable when the Type parameter is set to IP Address.

xiv Click on the OK button. The Prefix Option form closes and a dialog box appears.

xv Click on the OK button. The Prefix form reappears with Options tab displayed.

xvi Click on the OK button. The Prefix form closes and a dialog box appears.

xvii Click on the OK button. The IPv6 Address Pool form reappears with Prefixes tab displayed.

12 Click on the Options tab.

13 Click on the Create button. The IPv6 Address Pool Option form opens.

i Configure the parameters:

- Option
- Number
- Type
- Value
- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

The Number parameter is configurable when the Option parameter is set to Custom Option.

The Value parameter is configurable when the Type parameter is set to ASCII String, Hex String, or Domain.

The IP Address 1, IP Address 2, IP Address 3, and IP Address 4 parameters are configurable when the Type parameter is set to IP Address.

ii Click on the OK button. The IPv6 Address Pool Option form closes and a dialog box appears.

iii Click on the OK button. The IPv6 Address Pool form reappears with Options tab displayed.

14 Click on the OK button. The IPv6 Address Pool form closes and a dialog box appears.

15 Click on the OK button. The DHCPv6 Server form reappears with IPv6 Address Pool tab displayed.

16 Click on the OK button. The DHCPv6 Server form closes and a dialog box appears.

17 Click on the OK button. The Routing Instance form reappears.

18 Click on the OK button to save the configuration. A dialog box appears.

19 Click on the Yes button to verify the action.

20 Close the form.

Procedure 22-4 To perform a Force Partner Down action on a local DHCP server failover

The Force Partner Down action attempts to force a transition of the local DHCP server failover facility from a noCommunication state to a partnerDown state.

1 Choose Routing from the navigation tree view selector.

2 Navigate to the routing instance from which you want to perform a Force Partner Down action. Choose Network→NE→Routing Instance.

3 Right-click on the routing instance icon and choose Properties from the menu. The Routing Instance form opens with the General tab displayed.

4 Click on the Local DHCP Servers tab.

5 Click on the DHCPv4 or DHCPv6 sub-tab.

6 Select the DHCP server on which you want to perform a Force Partner Down action and click on the Properties button. The Local DHCP Server form opens.

7 Click on the Failover tab.

8 Click on the Force Partner Down button.

The fields in the Force Partner Down Action panel are updated to reflect the result of the Force Partner Down action.

9 Close the Local DHCP Server form.

10 Close the Routing Instance form.

Procedure 22-5 To configure a routing instance on an OmniSwitch

You can configure interfaces, routing protocols, and static routes on the default routing instances on all OmniSwitch NEs. See Procedure 22-1 to configure VRF instances on supported OmniSwitch NEs.

1 Choose Routing from the navigation tree view selector.

2 Navigate to a routing instance icon by choosing Network→NE→Routing Instance.

3 Right-click on the routing instance icon and choose Properties from the menu. The Routing Instance (Edit) form opens with the General tab displayed.

4 Click on the Routing tab.

5 Configure the Router ID parameter, if required.

6 Click on the Interfaces tab. See Procedure 22-11 for information about creating additional OmniSwitch L3 interfaces.

7 Click on the Address tab.

8 Configure IP address parameters for L3 interfaces.

i Choose an address in the list.

ii Click on the Properties button. The IP Address (Edit) form opens.

iii Configure the parameters, if required:

- IP Address
- Prefix Length

iv Click on the OK button to save the changes. A dialog box appears.

v Select the check box to indicate that you understand the implications of making the change or click on the No button and go to step ix.

vi Click on the Yes button. A dialog box appears.

vii Click on the Yes button. The Routing Instance (Edit) form reappears.

viii Go to step 9.

ix Close the IP Address (Edit) form.

9 Click on the Static Routes tab to view a list of static routes and to add static routes. See Procedure 22-14 for more information.

10 Click on the OK button to save the configuration. A dialog box appears.

11 Click on the Yes button to verify the action.

12 Close the form.

OmniSwitch DHCP relay and snooping

A DHCP relay agent is a BOOTP relay agent that relays DHCP messages between DHCP clients and DHCP servers on different IP networks. The Omniswitch supports global or per-VLAN BOOTP/DHCP relay service and per-VLAN UDP port relay services.

DHCP Option-82 and DHCP snooping provide security for a DHCP relay service. The DHCP Option-82 switch-level feature allows the relay agent to insert identifying information into client-originated DHCP packets before the packets are forwarded to the DHCP server. DHCP Snooping, at the switch or VLAN level, improves network security by filtering DHCP messages received from devices outside the network and building and maintaining a binding table to track access information for each device. DHCP relay Option-82 and snooping cannot be run on the switch at the same time.

DHCP relay and snooping is configured at the default routing instance level, see Procedure 22-6. In addition, per-VLAN DHCP snooping can be enabled on a VLAN site. See procedures 66-1, 66-2, and 66-3 for more information.

It is necessary to configure ports connected to DHCP servers within the network and/or firewall as trusted ports so that necessary DHCP traffic to/from the server is not blocked. Configuring the port mode as trusted also identifies the device connected to that port as a trusted device within the network. See Procedure 16-23 for more information.

Procedure 22-6 To configure a UDP relay service, DHCP snooping, and DHCP Option 82 on OmniSwitch routing instances



Note — For VRF instances on the OS 6850E, OS6855-U24X, OS 9700E, and OS 9800E NEs, only UDP Relay service is supported.

1 Choose Routing from the navigation tree view selector.

2 Navigate to an OmniSwitch routing instance by choosing Network→OmniSwitch → Routing Instance.



Warning 1 — The routing instance must be the default routing instance.

Warning 2 — UDP Server Statistics/UDP Service Statistics will be lost as part of the parent change from Bridge Instance to Routing Instance.

3 Right-click on the routing instance icon and choose Properties from the menu. The Routing Instance (Edit) form opens with the General tab displayed.

4 Click on the UDP Relay tab to configure UDP relay. The UDP Relay General Configuration tab is displayed.

5 Configure the following parameters in the UDP BOOTP/DHCP Relay General Configuration panel.

- Forwarding Delay (seconds)
- Maximum Hops
- Forwarding Option

6 If you need to use the DHCP Option-82 functionality, configure the following parameters in the Relay Information Configuration panel.

- Relay Agent Information Mode
- Relay Agent Information Policy

7 If you need support for PXE devices, configure the PXE Support parameter.



Note — For VRF instances on the OS 6850E, OS6855-U24X, OS 9700E, and OS 9800E NEs, the following parameters are read only:

- Forwarding Delay (seconds)
- Maximum Hops
- Relay Agent Information Mode
- Relay Agent Information Policy
- PXE Support

The values of these parameters are updated automatically if the corresponding value is modified under the default VRF instance.

8 Click on the DHCP Snooping tab to configure DHCP snooping.

9 Perform one of the following:

a If working on an OS 6900 or an OS 10K, configure the parameters:

- Option-82 Format Type
- ASCII Field 1 Format
- ASCII Field 2 Format
- ASCII Field 3 Format
- ASCII Field 4 Format
- ASCII Field 5 Format
- ASCII Delimiter
- Option-82 User String
- ASCII Field 1 String Value
- ASCII Field 2 String Value
- ASCII Field 3 String Value
- ASCII Field 4 String Value
- ASCII Field 5 String Value

b If working on a node other than an OS 6900 or an OS 10K, configure the parameters:

- DHCP Snooping Mode
- Bypass Option-82 Check
- Option-82 Format Type
- Option-82 User String
- MAC Address Verification
- Option-82 Data Insertion
- Binding Database Mode
- Synchronization Timeout (seconds)
- Action
- Binding Persistency

10 Configure UDP port relay services, if required. Click on the Relay Services tab.

11 Click on the Create button.

12 Configure the UDP Relay Service parameter.

If you selected the Other option, configure the Relay Service Port and Relay Service Description parameters.

13 Click on the OK button. A dialog box appears.

14 Click on the OK button.

15 Click on the Relay Destinations tab.

16 Click on the Create button. The Create UDP Service Destinations form opens with the Select Relay Service step displayed.

17 Click on the Select button. The Select UDP Service - UDP Relay Service Destination form opens.

18 Choose a UDP relay service. Click on the OK button.

19 If you selected BOOTP/DHCP (67/68) in step 18 and the parameter Forwarding Option is set to Standard, click on the Next button. Otherwise, go to step 22.

20 The Forwarding Address step is displayed.

21 Configure the Forwarding Address parameter, if required.

22 Click on the Next button. The Select VLANs step is displayed.

23 Configure the search filter and click on the Search button. The Select VLANs form displays the VLANs that match the search criteria.

24 Choose one or more VLANs to be used to forward the UDP traffic.

25 Click on the Finish button. The Create UDP Service Destinations form closes and the selected VLANs appear in the relay destinations list.

Procedure 22-7 To configure a RADIUS server on a routing instance

1 Choose Routing from the navigation tree view selector.

2 Navigate to a routing instance by choosing Network→NE→Routing Instance.

3 Right-click on the routing instance icon and choose Properties from the menu. The Routing Instance (Edit) form opens with the General tab displayed.

4 Click on the RADIUS tab.

5 Click on the Create button. The RADIUS Server (Create) form opens.

6 Configure the parameters:

- Name
- Address
- UDP Authentication Port
- UDP Accounting Port
- Secret
- Description
- Accept CoA
- Pending RADIUS Authentication Requests Limit

7 Click on the OK button. The RADIUS Server (Create) form closes and the Routing Instance (Edit) form reappears with the new RADIUS Server information displayed.

Procedure 22-8 To configure a RADIUS proxy server on a routing instance

1 Choose Routing from the navigation tree view selector.

2 Navigate to a routing instance by choosing Network→NE→Routing Instance.

3 Right-click on the routing instance icon and choose Properties from the menu. The Routing Instance (Edit) form opens with the General tab displayed.

4 Click on the RADIUS tab.

5 Click on the RADIUS Proxy Servers tab.

6 Click on the Create button. The RADIUS Proxy Server (Create) form opens with the general tab displayed.

7 Configure the parameters:

- Name
- Purpose
- Administrative State
- Description
- Secret
- Send Accounting Response

8 Click on the Select button in the Default RADIUS Server Policies Authentication panel. The Select Authentication - RADIUS Proxy Server form opens with a list of RADIUS server policies displayed.

9 Choose a RADIUS server policy and click on the OK button. The Select Authentication - RADIUS Proxy Server form closes and the RADIUS Proxy Server (Create) form reappears with the RADIUS server policy information displayed.

10 Click on the Select button in the Default RADIUS Server Policies Authorization panel. The Select Authorization - RADIUS Proxy Server form opens with a list of RADIUS server policies displayed.

11 Choose a RADIUS server policy and click on the OK button. The Select Authorization - RADIUS Proxy Server form closes and the RADIUS Proxy Server (Create) form reappears with the RADIUS server policy information displayed.

12 Configure the Key Type parameter.

13 If the Key Type parameter was set to Attributes, configure the parameters:

- Attribute Type 1
- Attribute Type 2
- Attribute Type 3
- Attribute Type 4
- Attribute Type 5
- Vendor ID 1
- Vendor ID 2
- Vendor ID 3
- Vendor ID 4
- Vendor ID 5

14 Click on the Caching tab.

15 Configure the parameters:

- Enable Caching
- Tracked Accounting Packets
- Packet Type

16 If the Packet Type parameter was set to any value other than None, configure the parameters:

- Attribute Type
- Vendor ID

17 Configure the Timeout parameter.

18 Click on the Interfaces tab.

19 Click on the Create button. The RADIUS Proxy Interface form opens.

20 Click on the Select button. The Select Interface - RADIUS Proxy Interface form opens with a list of interfaces displayed.

21 Choose an interface and click on the OK button. The Select Interface - RADIUS Proxy Interface form closes and the RADIUS Proxy Interface form reappears with the interface information displayed.

22 Click on the OK button. The RADIUS Proxy Interface form closes and the RADIUS Proxy Server (Create) form reappears with the interface information displayed.

23 Click on the OK button. The RADIUS Proxy Server (Create) form closes and the Routing Instance (Edit) form reappears with the new RADIUS Proxy Server information displayed.

Procedure 22-9 To create an L3 interface

The interfaces you can configure include the following:

- L3 network interface
- ICMP interface
- system interface
- management interface
- VRRP instance
- IGMP interface
- PIM interface
- MLD interface

1 Choose Routing from the navigation tree view selector.

2 Navigate to a routing instance by choosing Network→NE→Routing Instance.

3 Create an L3 interface by right-clicking on the routing instance icon and choosing Create Interface. The Create Network Interface step form opens.



Note — The steps that appear on the Create Network Interface step form depend on the device type, device version, and the options that are selected during configuration.

4 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- IPv6 Allowed
- MAC Address
- Allow Directed Broadcasts
- Class
- Loopback Enabled
- PIM RP Delayed Up Period
- Cflowd Type
- Trusted
- Admin Link Local Address
- Admin Link Local Address Preferred
- Strip Label
- Enable Ingress FlowSpec IPv4
- Enable Ingress FlowSpec IPv6
- Enable MAC Accounting Stats
- LDP Synchronization Timer
- FlowSpec Validate Enabled
- QoS Route Lookup IPv4
- QoS Route Lookup IPv6

5 Click on the Next button and perform one of the following:

a If you chose Numbered in the Class parameter in step 4, the Configure IP Address form opens. Specify the IP address information for the L3 interface:

i Click on the Create button. The IP Address (Create) form opens.

ii Configure the parameters:

- IP Address
- Prefix Length
- IGP Inhibit
- Broadcast Address Format
- EUI-64
- IP Address Preferred

The Broadcast Address Format parameter only appears if the IP Address parameter is set to an IPv4 address.

The EUI-64 and IP Address Preferred parameters only appear if the IP Address parameter is set to an IPv6 address.

iii Click on the OK button to save the changes. A dialog appears.

iv Click on the OK button. The IP Address (Create) form closes and the Configure IP Address form reappears.

b If you chose Unnumbered for the Class parameter in step 4, the Configure Unnumbered Interface form opens. Configure the parameters:

- Unnumbered Type
- Unnumbered Reference

6 Click on the Next button. The Select Port form opens.



Note — If the Loopback Enabled parameter is selected on the Define General Properties form, The Select Port step does not appear in the step menu for the 7950 XRS, 7450 ESS, 7750 SR, 7705 SAR, and 7710 SR.

7 Associate the L3 interface with a physical port.

i Click on the Select button. The Select Port form opens.

ii Choose a port.

iii Click on the OK button. The port is associated with the L3 interface.

8 Click on the Next button. The Select Network Policy form opens.

9 Click on the Select button in the Network Policy panel to list and choose a network policy for the interface. Network policies are used to determine QoS settings based on the packet DSCP bits on the ingress and egress of the network.



Note — If you select a network policy with a forwarding class mapped to a queue group queue ID, you must ensure that the mapping queue group queue ID is in the selected Queue Group Template Policy.

See Procedure 16-1 for more information about how to configure Ethernet ports. See chapter 42 for more information about queue group template policies.

10 In the Ingress Forwarding Plane Redirect panel:



Note 1 — You must ensure that the port you selected in step 7 has a network egress queue group with the same name as the Queue Group Template policy created on it.

Note 2 — If the Network Policy you selected in step 9 has Port Redirect Groups on its Ingress Forwarding Classes, you must specify both an Ingress Queue Group Template Policy and Instance ID.

Note 3 — If the Network Policy you selected in step 9 has Port Redirect Groups on its Egress Forwarding Classes, these must already be defined within the Egress Queue Group Template Policy you select.

Note 4 — Queue Group Template policies are not applicable to L3 interfaces associated with HSMDA ports.

See Procedure 16-1 for more information about how to configure Ethernet ports. See chapter 42 for more information about queue group template policies.

i Click on the Select button to choose a queue group template policy for the interface's ingress forwarding plane redirection. Only global Ingress Queue Group Template Policies that have already been defined can be chosen. Queue group template policies allow SAP or IP interface forwarding classes to be redirected from the typical queue mapping to a shared queue.

ii Configure the Queue Group Instance ID parameter.

11 In the Egress Port Redirect panel:



Note 1 — If the Network Policy you selected in step 9 has Port Redirect Groups on its Egress Forwarding Classes, you must specify both an Egress Queue Group Template Policy and Instance ID.

Note 2 — If the Network Policy you selected in step 9 has Port Redirect Groups on its Egress Forwarding Classes, these must already be defined within the Egress Queue Group Template Policy you select.

Note 3 — Queue Group Template policies are not applicable to L3 interfaces associated with HSMDA ports.

See Procedure 16-1 for more information about how to configure Ethernet ports. See chapter 42 for more information about queue group template policies.

i Click on the Select button to choose a queue group template policy for the interface's egress port redirection. Only local Egress Queue Group Template Policies which have a Network Egress Queue Group Instance defined on the associated port can be chosen.

ii Configure the Queue Group Instance ID parameter.

12 Click on the Next button. The Select ACL Filters form opens.

13 Click on the Select buttons to list and choose Ingress and Egress IPv4 and IPv6 ACL filters for the interface. ACL filters are used to filter out IP traffic that matches user-defined criteria.

14 Click on the Next button. The Configure ICMP form opens.

Configure the parameters:

- Mask Reply
- Redirects
- Unreachables
- TTL Expired
- Number of Redirects
- Redirects Time (seconds)
- Number of Unreachables
- Unreachables Time (seconds)
- Number of TTL Expired
- TTL Expired Time (seconds)

15 Click on the Next button. If the IPv6 Allowed parameter in step 4 is enabled, the Configure ICMPv6 form opens. Otherwise, go to step 16.

Configure the parameters:

- Redirects
- Unreachables
- Packet Too Big
- Param Problem
- Time Exceeded
- Number of Redirects
- Redirects Time (seconds)
- Number of Unreachables
- Unreachables Time (seconds)
- Number of Packet Too Big
- Packet Too Big Time (seconds)
- Number of Param Problem
- Param Problem Time (seconds)
- Number of Time Exceeded
- Time Exceeded Time (seconds)

16 Click on the Next button. The Configure ARP form opens.

i Configure the Timeout (seconds) parameter.

ii Click on the Create button to statically associate an IP or MAC address to the interface. The Static ARP (Create) form opens.

Configure the parameters:

- IP Address
- Physical Address

iii Click on the OK button. The Static ARP (Create) form closes.

17 Click on the Next button. The Configure Proxy ARP form opens.

Proxy ARP allows a device, such as a router, to answer ARP requests that are intended for another device. This allows a device to reach a remote subnet without configuring routes to the subnet or a default gateway device.

18 Configure the parameters:

- Remote Proxy ARP
- Enable Local Proxy ARP

19 Click on the Next button. The Configure Proxy ARP Policies form opens.

20 Configure the parameters:

- Proxy Arp Policy 1
- Proxy Arp Policy 2
- Proxy Arp Policy 3
- Proxy Arp Policy 4
- Proxy Arp Policy 5

21 Click on the Next button. If the IPv6 Allowed parameter in step 4 is enabled, the Configure Neighbor Discovery form opens. Otherwise, go to step 27.

22 Click on the Create button to configure a neighbor. The Neighbor Discovery (Create) form opens.

23 Configure the parameters:

- IP Address
- Physical Address

24 Click on the OK button. The Neighbor Discovery (Create) form closes and the Configure Neighbor Discovery form reappears.

25 Click on the Next button. The Configure Proxy Neighbor Discovery form opens.

26 Configure the parameters:

- Enable Local Proxy
- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5



Note — You must not leave an empty policy parameter between two configured policy parameters. For example, do not configure the Policy 1 and Policy 3 parameters and leave the Policy 2 parameter unconfigured. The 5620 SAM reorders the policies and moves the policy entered for the Policy 3 parameter to the Policy 2 parameter.

27 Click on the Next button. The Configure NTP form opens.

28 Configure the Broadcast parameter.



Note — When the Broadcast parameter is enabled, a time protocol such as NTP or SNTP must be enabled and configured on the device, or the device ignores broadcast time packets received on the interface. See chapter 9 for information about configuring NTP or SNTP on a device.

29 Click on the Next button. The Configure DHCP - General form opens.

30 Configure IPv4 DHCP for the interface, if required.

i Configure the parameters:

- Enable DHCP Relay
- Description
- Action
- Circuit ID
- Remote ID
- Remote ID String
- Copy To Option 43



Note — The Remote ID String parameter is configurable when the Remote ID parameter is set to Remote IDString.

ii Click on the Next button. The Configure DHCP - Server form opens.

iii Configure the Server 1 through Server 8 parameters.

31 Click on the Next button. The Configure VRRP form opens.

VRRP instances are members of a virtual router that provides backup if a router fails in a statically configured LAN. VRRP instances are created from network interfaces on a router, either as a master owner through which IP packets are routed before a failover or as a backup non-owner that assumes the packet-forwarding (master) role after a failover. Before you create or add a VRRP instance to a virtual router, ensure that the master and backup interfaces have the same VRID and occupy the same subnet.

32 Perform one of the following:

a If a VRRP instance is not required, click on the Next button until the Unicast RPF form opens in step 41.

b If an IPv4 VRRP instance is required, click on the Create button. The VRRP Instance (Create) form opens with the General tab displayed. See chapter 33 for information about VRRP instances and virtual routers.

c If an IPv6 VRRP instance is required, click on the Next button. The Configure IPv6 VRRP form is displayed. Click on the Create button and the VRRP IPv6 Instance (Create) form opens with the General tab displayed. See chapter 33 for information about VRRP instances and virtual routers.

33 Click on the Next button. The Configure Router Advertisement form opens.

34 Click on the Create button to add a router advertisement entry. The Router Advertisement (Create) form opens with the General tab displayed.

35 Configure the parameters:

- Send Advertisement
- Min Interval (seconds)
- Reachable Time (milliseconds)
- Managed Address Config
- MTU
- Use Virtual MAC Address
- Max Interval (seconds)
- Retransmit Time (milliseconds)
- Other Stateful Config
- Current Hop Limit
- Lifetime (seconds)

If you are configuring the L3 interface for an IPv6 VRRP instance, then the Send Advertisement and Use Virtual MAC Address parameters must both be enabled.

36 Click on the Prefix tab.

37 Click on the Create button. The Router Advertisement Prefix (Create) form opens.

38 Configure the parameters:

- IPv6 Prefix
- Prefix Length
- On-Link Determination
- Autonomous Address Configuration
- Lifetime (seconds)
- No Expiry
- Lifetime (seconds)
- No Expiry



Note — Each Lifetime (seconds) parameter is configurable when the associated No Expiry parameter is disabled.

39 Click on the OK button. A dialog box appears.

40 Click on the OK button. The Router Advertisement Prefix (Create) form closes.

41 Click on the Next button. The Unicast RPF form opens.

42 Configure the parameters:

- URPF Check State IPv4
- URPF Check Mode IPv4
- URPF Check State IPv6
- URPF Check Mode IPv6

The URPF Check State IPv6 and URPF Check Mode IPv6 parameters are only configurable when the IPv6 Allowed parameter is enabled.

43 Click on the Next button. The Configure Network Domain form opens.

44 Configure the parameters. You can Add Network Domain or Remove Network Domain.

45 Click on the Next button. The Configure BFD form opens.

46 Configure Bidirectional Forwarding Detection for the interface, if required.

i Set the Administration Status parameter to Up. The configuration form is refreshed with additional parameters.

ii Configure the parameters:

- Administration Status
- Transmit Interval
- Receive Interval
- Echo Interval
- Multiplier
- Termination Type
- Operational State Transition Interval
- Inherit from Network Element

iii To view local and remote session peers, click on the BFD Session tab. 5620 SAM retrieves information from local and remote nodes and displays a list of BFD current sessions on router interfaces or L3 interfaces.

iv Click on a session. A properties window opens for the session. View the following:

- BFD status
- protocol used
- local address
- remote address
- operational status and statistics

The BFD Status field indicates one of the following:

- “no service”, when BFD is disabled
- “in service”, when BFD is running
- “out of service”, when BFD has failed

v Click on the OK button.



Note — You cannot enable BFD on an interface, if BFD is not configured on the interface. You cannot set the administration status of an interface to disabled, when protocols using the interface have BFD enabled. See chapter 23 for information about enabling and disabling BFD for routing protocols.

47 Click on the Next button. If the IPv6 Allowed parameter in step 4 is enabled, the Configure IPv6 BFD form opens and you can configure IPv6 BFD parameters for the interface as in step 52.

48 Click on the Finish button. The Summary form opens.

49 Enable the View the newly created Network Interface parameter to view the interface configuration after closing the form, if required.

50 Click on the Close button. The Create Network Interface step form closes.

51 If the View the newly created tunnel parameter in step 49 is enabled, the Network Interface (Edit) form opens with the newly created interface configuration displayed. To configure BFD on the network interface, go to step 52.

52 Configure Bidirectional Forwarding Detection for the interface, if required.

i Click on the BFD tab. A configuration form opens.

ii Set the Administration Status parameter to Up. The configuration form is refreshed with additional parameters.

iii Configure the parameters:

- Administration Status
- Transmit Interval
- Receive Interval
- Echo Interval
- Multiplier
- Termination Type
- Inherit from Network Element
- Operational State Transition Interval

iv To view local and remote session peers, click on the BFD Session tab. 5620 SAM retrieves information from local and remote nodes and displays a list of BFD current sessions on router interfaces or L3 interfaces.

v Click on a session. A properties window opens for the session. View the following:

- BFD status
- protocol used
- local address
- remote address
- operational status and statistics

The BFD Status field indicates one of the following:

- “no service”, when BFD is disabled
- “in service”, when BFD is running
- "out of service", when BFD has failed

vi Click on the OK button.



Note — You cannot enable BFD on an interface, if BFD is not configured on the interface. You cannot set the administration status of an interface to disabled, when protocols using the interface have BFD enabled. See chapter 23 for information about enabling and disabling BFD for routing protocols.

Procedure 22-10 To configure an L3 interface

This procedure describes how to configure L3 interface parameters. The interfaces you can modify include the following:

- L3 network interface
- ICMP interface
- system interface
- management interface
- VRRP instance
- IGMP interface
- PIM interface
- MLD interface

1 Choose Routing from the navigation tree view selector.

2 Navigate to a network interface. The path is Routing→NE→Routing Instance→Interface.

3 Choose an interface and choose Properties from the menu. The Network Interface (Edit) form opens.

4 Click on the appropriate tab and configure the parameters, if required. Table 22-4 describes the tabs to choose, as shown when you modify an existing routing interface.

Table 22-4 Description of network interface configuration form tabs

Tab	Description
General	Configure the parameters: • Description • Administrative State • IPv6 Allowed • MAC Address • Allow Directed Broadcasts • Class • Loopback Enabled • PIM RP Delayed Up Period • Cflowd Type • Trusted • LDP Synchronization Timer • Enable Ingress FlowSpec • Enable Ingress FlowSpec IPv6 • PTP HW Assist
Port	To create an association between the L3 interface and a physical port or channel. The system interface is not associated with a port.
Policies	To associate network policies and ingress or egress IP ACL filter policies with the network interface.
Protocols	To view a list of protocols that are enabled on the interface, and to apply protocols. The protocols are: • MPLS • OSPFv2 • OSPFv3 • LDP • IS-IS • RIP
Multicast	To view a list of multicast protocols that are enabled on the interface, and to apply protocols. The protocols are: • PIM • IGMP • MLD
Local DHCP Servers	To assign local DHCP servers. Local DHCP servers are configured on the routing instance and VPRN service. They must be assigned to a network or an L3 interface. To assign local DHCPv6 servers the IPv6 Allowed parameter must be enabled.
DHCP Client	To enable a DHCP Client on a network interface, configure the parameters: • Enable DHCP Client • Client Identifier • Vendor Class ID
Security	To assign a DoS protection policy or DDoS protection policy to a network interface.
RCA Result	To view the results of RCA activities on the network interface
Address	To assign an IP address, subnet and broadcast address format to a network interface. Only one primary IP address can be associated with a network interface.
BFD	To configure BFD parameters

(1 of 2)

Tab	Description
ARP	To configure or view ARP and proxy ARP parameters. Click on the General tab to configure the minimum time, in seconds, that an ARP entry is stored in the ARP table. Click on the Create button to configure static ARP IP and MAC address parameters. Click on the Proxy ARP tab to view parameter information.
ICMP	To configure ICMP parameters
ICMPv6	If IPv6 is enabled on the interface, to configure ICMPv6 parameters
Neighbor Discovery	To configure neighbor discovery and proxy neighbor discovery for static routes. Click on the General tab and Create button to configure neighbor discovery IP and MAC address parameters. Click on the Proxy ND tab to configure proxy neighbor discovery parameters. (1)
VRRP	To add a VRRP instances to an existing virtual router that assumes routing responsibilities from a failed router in a statically configured LAN
MEPs	To add network interface facility MEPs. Each network interface can support one facility MEP. • To perform continuity messaging on the network interface facility MEP, enable the CCM Messages Enabled parameter. • To enable fault propagation on the network interface facility MEP, enable the Facility Fault Notify parameter.
Advertisement	To configure router advertisement
DHCP	To configure DHCP Relay parameters
NTP	To enable SNTP broadcasts on the network interface
Statistics	To view L3 network interface statistics
Faults	To view alarms that are raised against the network interface, or related alarms that affect the network interface

(2 of 2)

Note
(1) The Proxy ND tab is available only on the 7750 SR.

5 Click on the Apply button to save the changes.

6 Close the form.

7 Cable the network ports or channels of the device, with L3 interfaces enabled, to other devices configured the same way.

8 Configure routing protocols, as described in chapter 23.

Procedure 22-11 To create a L3 interface on an OmniSwitch

An L3 interface enables IP routing on a VLAN. Without an L3 interface, traffic is bridged within the VLAN or across connections to the same VLAN on other switches.

1 Choose Routing from the navigation tree view selector.

2 Navigate to an OmniSwitch routing instance by choosing Network→OmniSwitch →Routing Instance.

3 Right-click on the routing instance icon and choose Create Interface from the menu. The Create Network Interface step form opens with the Define General Properties form displayed.

4 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- Configured Primary Status
- Enable Forwarding

5 Click on the Next button. The Configure IP Address form opens.

6 Click on the Create button. The IP Address (Create) form opens.

7 Configure the parameters:

- IP Address
- Prefix Length

8 Click on the OK button. The IP Address (Create) form closes and a dialog box appears.

9 Click on the OK button.

10 Click on the Next button. The Configure Proxy ARP form opens.

11 Configure the Enable Local Proxy ARP parameter.

12 Click on the Next button. The Select VLAN form opens.

13 Click on the Select button. The Select VLAN - Network Interface form opens.

14 Choose a VLAN to which you need to add the interface.

15 Click on the OK button. The Select VLAN - Network Interface form closes.

16 Click on the Finish button. The Summary form opens.

17 Select the View the newly created Network Interface parameter to view the interface configuration after you close the Summary form, if required.

18 Click on the Close button. The Create Network Interface step form closes.

Procedure 22-12 To configure L3 interfaces on an OmniSwitch

1 Choose Routing from the navigation tree view selector.

2 Navigate to a network interface by choosing Network→ OmniSwitch →Routing Instance→Interface.

3 Choose an interface and choose Properties from the menu. The Network Interface (Edit) form opens.

4 Click on the appropriate tab and modify the parameters, if required. Table 22-5 describes the tabs.

Table 22-5 Description of OmniSwitch network interface configuration form tabs

Tab	Description
General	Configure the parameters: • Description • Administrative State • Configured Primary Status • Enable Forwarding • Encap Type
VLAN	View properties of the VLAN to which the interface is assigned or assign a VLAN to the interface.
Address	Assign an IP address to a network interface or view properties of an assigned address. Only one primary IP address can be associated with a network interface.
ARP	Configure the Enable Local Proxy ARP parameter.
Faults	View alarms that are raised against the network interface, or related alarms that affect the network interface.

5 Click on the Apply button to save the changes.

6 Close the form.

Procedure 22-13 To create a static route

1 Choose Routing from the navigation tree view selector.

2 Navigate to the static routes icon. The navigation path is Routing→NE→Routing Instance→Static Routes.

3 Right-click on the static routes icon and choose Create Static Route from the menu. The Static Route (Create) form opens.

4 Configure the parameters:

- Auto-Assign ID
- Static Route ID
- BFD Enabled
- Forwarding Class Name
- Forwarding Class Priority
- Community
- Description
- Destination
- Prefix Length
- Multicast Capable Peers
- Dynamic BGP
- Type
- IP Address
- Interface Name
- Unnumbered Interface
- Preference
- Metric
- Administrative State
- Tag
- LDP
- Disallow IGP
- Enable CPE Check
- Target IP Address
- Interval (seconds)
- Drop Count
- Log
- Prefix List Name
- Prefix List Flag
- Packet Size

The Dynamic BGP parameter is configurable when the Type parameter is set to Black Hole.

The IP Address parameter is configurable when the Type parameter is set to an option other than Black Hole.

The Target IP Address, Interval (seconds), Drop Count, and Log parameters are displayed only when Enable CPE Check is enabled.

You cannot specify a Prefix List if either BFD Enabled or Enable CPE Check parameters are enabled for the static route.

The Prefix List Flag Prefix List Name parameter is configured.

5 If IPv6 is enabled on the routing instance, click on the Select button beside the Interface Name parameter to choose an IPv6 zone index for the static route. The Select Zone Index - Static Route form opens. Otherwise, go to step 7.

6 Choose a zone index in the list and click on the OK button. The Select Zone Index - Static Route form closes and the zone index is displayed in the Static Route (Create) form.

7 Click on the OK button. The Static Route (Create) form closes.

Procedure 22-14 To configure a static route on an OmniSwitch

1 Choose Routing from the navigation tree view selector.

2 Navigate to the static routes icon by choosing Network→OmniSwitch or→Routing Instance→Static Routes.

3 Right-click on the static routes icon and choose Create Static Route from the menu. The Static Route (Create) form opens.

4 Configure the parameters:

- Auto-Assign ID
- Static Route ID
- Destination
- Prefix Length
- Type
- IP Address
- Metric



Note — If the address entered for the IP Address parameter is unreachable by the node, the static route is not created on the node. Use the 5620 SAM to verify that all configured static routes are created successfully on the node by checking the list of static routes for the OmniSwitch routing instance.

5 Click on the OK button to save the configuration. The Static Route (Create) form closes.

Procedure 22-15 To configure a routing policy statement

See "Routing policies" in section 22.1 for more information about routing policies.

1 Choose Policies→Routing→Statement from the 5620 SAM main menu. A Routing Policy Statement Manager form opens.

2 Click on the Create button.

3 Configure the parameters:

- Policy Statement Name
- Description
- Default Action
- Check Dependencies



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Perform one of the following:

a Click on the Components tab. Choose and right-click on Policy Statement Entry and choose Create Policy Statement Entry. The Policy Statement Entry (Create) form opens with the General tab displayed. Go to step 6.

b Click on the Policy Statement Entries tab.

5 Click on the Create button. The Policy Statement Entry (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Entry ID
- Description
- Action

7 Perform one of the following:

a If you choose Accept, Next Entry, or Next Policy for the Action parameter, go to step 8.

b If you choose None or Reject for the Action parameter, go to step 19.

8 Click on the Action tab. The General sub-tab under the General tab is displayed.

9 Configure the parameters:

- Route Origin
- Route Preference
- BGP Local Preference
- Local Preference Set
- Use Next Hop
- OSPF Route Type
- Advertise Next Hop Self
- Accumulated IGP Metric Value
- Accumulated IGP Metric
- Metric Value
- Metric Action
- Metric Source
- OSPF, RIP, or ISIS Tag (Hex)
- Next Hop Type
- Damping Profile Name
- Interface
- Forwarding Class Name
- Forwarding Class Priority

10 Click on the Path sub-tab.

11 Configure the parameters:

- BGP AS Path Name
- BGP AS Path Action
- BGP AS Prepend number
- Prepend Count

12 Click on the BGP Community sub-tab.

13 Configure the parameters:

- Community Name 1
- Community Action 1
- Community Name 2
- Community Action 2

14 Click on the Community Actions sub-tab.

15 Click on one of the Add, Remove, or Replace sub-tab to perform the specific action that you want to perform.



Note — In the Community Actions context, the Add/Remove and Replace actions are mutually exclusive.

16 Click the Select button. The Select Policy Statement Entry form opens.

17 Click the Search button and select the required entry from the list.

18 Click OK. The Select Policy Statement Entry form closes and your selection appears in the Community Name Action field of the tab you selected in step 15.

19 Click on the From Criteria tab. The General sub-tab displayed.

20 Click on the Select button beside the AS Path Name parameter. The Select Policy Statement Entry - Site form opens.

21 Choose an AS Path from the list and click on the OK button. The AS Path Name is refreshed with the selected AS Path.

22 Click on the Select button beside the AS Path Group Name parameter. The Select Policy Statement Entry - Site form opens.

23 Choose an AS Path Group from the list and click on the OK button. The AS Path Group Name is refreshed with the selected AS Path Group.

24 Click on the Select button beside the Community List Name parameter. The Select Policy Statement Entry - Site from opens.



Note — Selecting a Community List Name in this step is mutually exclusive with creating a Community List Expression in step 39.

25 Choose a community and click on the OK button. The Community List Name is refreshed with the selected community.

26 Configure the parameters.

- Protocol
- Origin
- State
- Interface Name
- Static Route Tag
- No Route Tag
- Family
- Level
- IS-IS External Route
- OSPF Route Type
- OSPF Area
- OSPF Area Set
- Multicast Source IP Address
- Neighbor IP Address

27 Perform the following to add sub-policy calls to group match criteria over multiple policy entries for complex match conditions. Any match conditions that are above the sub-policy are evaluated first. If all of the match conditions are met, the sub-policy is evaluated.



Note — You cannot add policies that have nested sub-policies.

i Click on the Select button beside the Policy Statement Name parameter. The Select Policy Statement Entry form opens. Alternatively, enter a policy name and go to step 28.

ii Choose a policy and click on the OK button. The Policy Statement Name parameter is refreshed with the selected policy.

28 Click on the Select button beside the Multicast Group Prefix List Name parameter. The Select Policy Statement Entry form opens.

29 Choose a policy and click on the OK button. The Multicast Group Prefix List Name parameter is refreshed with the selected policy.

30 Click on the Select button beside the IGMP Host Prefix List Name parameter. The Select Policy Statement Entry form opens.

31 Choose a policy and click on the OK button. The IGMP Host Prefix List Name parameter is refreshed with the selected policy.

32 Click on the Select button beside the Interface Name parameter. The Select Zone Index From Criteria Site form opens.

33 Choose a site and click on the OK button. The Interface Name parameter is refreshed with the selected site.

34 Click on the Select button beside the Neighbor Prefix List Name parameter. The Select Policy Statement Entry form opens.

35 Choose a policy statement and click on the OK button. The Neighbor Prefix List Name parameter is refreshed with the selected policy.

36 Click on the Prefix List tab.

37 Configure the parameters.

- Prefix List 1
- Prefix List 2
- Prefix List 3
- Prefix List 4
- Prefix List 5

38 Click on the Community Expression sub-tab.

39 Create a Community List Expression.



Note — Creating a Community List Expression in this step is mutually exclusive with selecting a Community List Name in step 24.

You enter pre-defined Community lists here which become part of a defined Community List Expression. You then use Boolean operators to define the policy's actions between different lists. Valid expression operators include: AND, OR, and NOT. The Boolean operators can also be used with parentheses and combined into a more complex expression. For example:

```
[comlist1] AND ([comlist3] OR [comlist4])
```



Note — When constructing a Community List Expression, Community Names must be limited to 32 characters maximum, and are enclosed within square parentheses. The entire Community List Expression must be limited to 900 characters maximum.

i Click on the Create button. A Community Expression (Create) form opens

ii Click the Select button. The Select Community form opens.

iii Click the Search button and choose an entry from the list, then click OK.

The Select Community form closes and the entry you selected appears in the Community Name field.

iv Click the Add button to place the entry into the Community List Expression field.

v Construct the Community List Expression string as required by adding other Community Names and connecting them with the appropriate Boolean operators and parentheses. The operators and parentheses are added to the expression by clicking on the required button below the Community List Expression field.

vi If you make an error in the construction of the string, you can use the Clear All button to start again, or just place your cursor in the field and do a manual editing correction.

vii Click on the OK button. A dialog box appears.

viii Click on the OK button. The Community Expression (Create) form closes and the Policy Entry Statement (Create) form is updated with the newly created expression.

ix Repeat steps i to viii to add other Community List Expressions, as required.

40 Click on the To Criteria tab. The Policy Statement Entry (Create) form opens with the General tab displayed.

41 Configure the parameters.

- Protocol
- Instance ID
- All Instances
- Level
- Neighbor IP Address

42 Click on the Select button beside the Neighbor Prefix List Name parameter. The Select Policy Statement Entry form opens.

43 Choose a policy.

44 Click on the OK button. The Neighbor Prefix List parameter is refreshed with the selected policy.

45 Click on the Select button beside the Interface Name parameter. The Select Zone Index To Criteria Site form opens.

46 Choose an interface.

47 Click on the OK button. The Interface Name parameter is refreshed with the selected site.

48 Click on the Prefix Lists tab.

49 Configure the parameters.

- Prefix List 1
- Prefix List 2
- Prefix List 3
- Prefix List 4
- Prefix List 5

50 Click on the OK button. A dialog box appears.

51 Click on the OK button.

Note — A routing policy is discovered as local edit only. To synchronize a routing policy with all NEs, you must change the distribution mode of the routing policy to sync with global. To configure the distribution mode, see Procedure 42-1.

52 Configure the following routing-related policies, if required:

a To configure a prefix list policy, see Procedure 22-16.

b To configure a community policy, see Procedure 22-17.

c To configure a damping policy, see Procedure 22-18.

d To configure an AS Path policy, see Procedure 22-19.

e To configure an AS Path Group policy, see Procedure 22-20.

f To view a routing policy from a CLI session, see Procedure 22-29.

Procedure 22-16 To configure a prefix list policy

See "Routing policies" in section 22.1 for more information about the use and purpose of routing policies.

1 Choose Policies→Routing→Prefix List from the 5620 SAM main menu. A Routing Policy Prefix List Manager form opens.

2 Click on the Create button. The Routing Policy Prefix List (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Prefix List Name
- Description



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Prefix List Members tab.

5 Click on the Create button. The Prefix List Member (Create) form opens.

6 Configure the parameters:

- Prefix
- Mask
- Type
- Begin Length
- Through Length
- Description

The Begin Length and Through Length parameters are configurable when the Type parameter value is set to Range or Through.

7 Click on the OK button. A dialog box appears.

8 Click on the OK button. The Routing Policy Prefix List, Global Policy (Create) form opens with the newly created prefix member.

9 Close the Routing Policy Prefix List, (Create) form.



Note — A routing policy is discovered as local edit only. To synchronize a routing policy with all NEs, you must change the distribution mode of the routing policy to sync with global. To configure the distribution mode, see Procedure 42-1.

10 Configure the following routing-related policies, if required:

a To configure a policy statement, see Procedure 22-15.

b To configure a community policy, see Procedure 22-17.

c To configure a damping policy, see Procedure 22-18.

d To configure an AS Path policy, see Procedure 22-19.

e To configure an AS Path Group policy, see Procedure 22-20.

f To view a routing policy from a CLI session, see Procedure 22-29.

Procedure 22-17 To configure a community policy

See "Routing policies" in section 22.1 for more information about the use and purpose of routing policies.

1 Choose Policies→Routing→Community from the 5620 SAM main menu. A Manage Routing Policy - Community form opens.

2 Click on the Create button. A Routing Policy - Community, Global Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Community Name
- Description

4 Perform one of the following:

a To create a Community Expression, go to step 5.

b To create a Community Member, go to step 9.

5 Click on the Community Expression tab.

6 Click on the Create button. A Community Expression (Create) form opens.

You can enter a string here which becomes a defined Community Expression. You use Boolean operators to define the policy's actions between different values. Valid expression operators include: AND, OR, and NOT. For example, if you enter the following string:

```
target:5:1000 OR target:9:10
```

then the policy matches a route that has either target. Or if you enter:

```
2:2 AND 200:200
```

then the policy only matches a route that has both targets.

The Boolean operators can also be used with parentheses and combined into a more complex expression, such as:

```
(8:8 AND NOT 9:9) OR (7:7)
```

In this case, the policy matches a route which contains the regular expression for target 8:8 with the exception of target 9:9, or just target 7:7 alone.

Any community (including a regular expression), extended community (including a regular expression) or well-known community can be part of the Community Expression. Therefore, valid values for the Community Expression's components include:

- Community Values, such as 100:100
- Extended Community Values, such as target:1:1, origin 1:1, target:1.1.1.1:1, or origin 1.1.1.1:1
- Regular expressions for communities, such as 100|200:100|200
- Regular expressions for extended community values



Note — When constructing a Community Expression, Community IDs must be limited to 75 characters maximum, and regular expressions must be limited to 72 characters maximum. The entire Community Expression must be limited to 900 characters maximum.

Community Expressions are supported on the 7750 SR, 7750 SR-c12, 7750 SR-12E, 7710 SR, and 7450 ESS. IOM3 is required, in chassis mode B, C, or D.

7 Click the OK button. The Community Expression (Create) form closes and the Routing Policy Community (Create) form is updated with the newly created Community Expression.

8 Go to step 14.

9 Click on the Community Members tab.

10 Click on the Create button. A Community Member Site (Create) form opens.

11 Configure the Community Member parameter.

12 Click on the OK button. A dialog box appears.

13 Click on the OK button. The Routing Policy Community (Create) form is updated with the newly created site.

14 Close the Routing Policy - Community, Global Policy (Create) form.

15 Close the Manage Routing Policy - Community form.



Note — A routing policy is discovered as local edit only. To synchronize a routing policy with all NEs, you must change the distribution mode of the routing policy to sync with global. To configure the distribution mode, see Procedure 42-1.

16 Configure the following routing-related policies, if required:

a To configure a policy statement, see Procedure 22-15.

b To configure a prefix list policy, see Procedure 22-16.

c To configure a damping policy, see Procedure 22-18.

d To configure an AS Path policy, see Procedure 22-19.

e To configure an AS Path Group policy, see Procedure 22-20.

f To view a routing policy from a CLI session, see Procedure 22-29.

Procedure 22-18 To configure a damping policy

See "Routing policies" in section 22.1 for more information about the use and purpose of routing policies.

1 Choose Policies→Routing→Damping from the 5620 SAM main menu. A Manage Routing Policy - Damping form opens.

2 Click on the Create button. A Routing Policy - Damping, Global Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Damping Name
- Half Life
- Reuse
- Suppress
- Max Suppression



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the OK button.

5 Close the Routing Policy - Damping, Global Policy (Create) form.



Note — A routing policy is discovered as local edit only. To synchronize a routing policy with all NEs, you must change the distribution mode of the routing policy to sync with global. To configure the distribution mode, see Procedure 42-1.

6 Configure the following routing-related policies, if required:

a To configure a policy statement, see Procedure 22-15.

b To configure a prefix list policy, see Procedure 22-16.

c To configure a community policy, see Procedure 22-17.

d To configure an AS Path policy, see Procedure 22-19.

e To configure an AS Path Group policy, see Procedure 22-20.

f To view a routing policy from a CLI session, see Procedure 22-29.

Procedure 22-19 To configure an AS Path policy

See "Routing policies" in section 22.1 for more information about the use and purpose of routing policies.

1 Choose Policies→Routing→AS Path from the 5620 SAM main menu. A Manage Routing Policy - AS Path form opens.

2 Click on the Create button. An Routing Policy - AS Path, Global Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Path Name
- Description
- Regular Expression



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the OK button.



Note — A routing policy is discovered as local edit only. To synchronize a routing policy with all NEs, you must change the distribution mode of the routing policy to sync with global. To configure the distribution mode, see Procedure 42-1.

5 Configure the following routing-related policies, if required:

a To configure a policy statement, see Procedure 22-15.

b To configure a prefix list policy, see Procedure 22-16.

c To configure a community policy, see Procedure 22-17.

d To configure a damping policy, see Procedure 22-18.

e To configure an AS Path Group policy, see Procedure 22-20.

f To view a routing policy from a CLI session, see Procedure 22-29.

Procedure 22-20 To configure an AS Path Group policy

See "Routing policies" in section 22.1 for more information about the use and purpose of routing policies.

1 Choose Policies→Routing→AS Path Group from the 5620 SAM main menu. The Manage Routing Policy - AS Path Groups form opens.

2 Click on the Create button. The Routing Policy - AS Path Group (Create) form opens with the General tab displayed.

3 Configure the parameters:

- AS Path Group Name
- Description



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the AS Path Group Entries tab.

5 Click on the Create button. The AS Path Group Entry (Create) form opens.

6 Configure the parameters:

- Auto-Assign ID
- Entry ID
- Regular Expression

If the Regular Expression you enter is invalid, then the OK and Apply buttons are disabled.

Note — You must create at least one AS Path Group Entry for this policy.

7 Click on the Apply button.

Note — A routing policy is discovered as local edit only. To synchronize a routing policy with all NEs, you must change the distribution mode of the routing policy to sync with global. To configure the distribution mode, see Procedure 42-1.

Once the policy has been successfully distributed, the local definitions can be viewed by clicking the Local Definitions tab.

8 Configure the following routing-related policies, as required:

a To configure a policy statement, see Procedure 22-15.

b To configure a prefix list policy, see Procedure 22-16.

c To configure a community policy, see Procedure 22-17.

d To configure a damping policy, see Procedure 22-18.

e To configure an AS Path policy, see Procedure 22-19.

f To view a routing policy from a CLI session, see Procedure 22-29.

Procedure 22-21 To configure an MPLS administrative group policy

MPLS administrative group policies define administrative groups that can be assigned to MPLS interfaces, LSPs, and LSP paths. After you configure MPLS administrative groups, the administrative groups can be assigned to MPLS interfaces, LSPs, and LSP paths on their respective properties forms. Multiple administrative groups can be assigned to each of these objects.

When establishing LSP and LSP paths, devices are only consider MPLS interfaces which are associated with the same administrative group as the LSP or LSP path. MPLS interfaces advertise administrative group associations using CSPF. This is done using the 32 bit mask which you configure using the Value parameter on the MPLS administrative group policy form.

An administrative group can also be assigned to be explicitly excluded from LSPs and LSP paths. The device cannot use MPLS interfaces in the administrative group to establish LSPs or LSP paths. Administrative group exclusion takes priority over administrative group inclusion.

CSPF must be enabled on LSPs for administrative groups to be relevant. You can enable and configure CSPF on the LSP properties form. When CSPF is enabled on an LSP, it is automatically enabled on associated LSP paths. LSP paths can be configured on the LSP path properties form to inherit additional CSPF, administrative group, and other parameters from LSPs.

This procedure describes how to create MPLS administrative groups. Table 22-6 describes where to find information about assigning MPLS administrative groups to MPLS interfaces, LSPs, and LSP paths.

Table 22-6 MPLS administrative group assignments

To assign groups to	See Procedure
MPLS interfaces	"To create an MPLS interface" in chapter 25
LSPs	"To create a static LSP" in chapter 25
LSP paths	"To configure an LSP path" in chapter 25

1 Choose Policies→MPLS→MPLS Administrative Group from the 5620 SAM main menu. The Manage MPLS Administration Groups form opens.

2 Click on the Create button. The Admin Group (MPLS) Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Value



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Apply button to save the policy.

The Admin Group (MPLS) Policy (Edit) form is refreshed and the tabs are selectable. Table 22-7 describes the tabs that you can choose to configure the parameters.

Table 22-7 Description of MPLS administrative group form tabs

Tab	Description
Local Definitions	Lists MPLS administrative group policies and allows you to manage administrative group policy distribution.
LSPs	Lists and allows you to manage LSPs to which the administrative group has been assigned.
LSP-Path Bindings	Lists and allows you to manage LSP paths to which the administrative group has been assigned.
Interfaces	Lists and allows you to manage MPLS interfaces to which the administrative group has been assigned.
Faults	List and manage alarms related to the administrative group.

5 Click on the Distribute button to manually distribute the administrative group policy locally to managed devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to managed devices when they are used by resources on the device.

Procedure 22-22 To configure a Shared Risk Link Group policy

This procedure describes how to create SRLG policies. Table 22-8 describes where to find information about related MPLS and LSP procedures.

Table 22-8 Related MPLS and LSP procedures

To:	See Procedure:
Configure an MPLS instance	"To configure an MPLS instance" in chapter 25
Create an MPLS interface	"To create an MPLS interface" in chapter 25
Configure LSP paths	"To configure an LSP path" in chapter 25

1 Choose Policies→MPLS→Shared Risk Link Group from the 5620 SAM main menu. The Manage Shared Risk Link Group Policies form opens.

2 Click on the Create button.

The Shared Risk Link Group, Global Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Value



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Apply button to save the policy.

The Shared Risk Link Group Policy (Edit) form is refreshed and the tabs are selectable. Table 22-9 describes the tabs that you can choose to configure the parameters.

Table 22-9 Description of Shared Risk Link Group Policy form tabs

Tab	Description
General	Displays information on the policy and allows you to prepare the policy for release and distribution.
Local Definitions	Lists Shared Risk Link Group policies and allows you to manage policy distribution.
Interfaces	Lists and allows you to manage MPLS interfaces to which the SRLG policy has been assigned.
Faults	List and manage alarms related to the SRLG.

5 Click on the Distribute button to manually distribute the SRLG policy locally to managed devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to managed devices when they are used by resources on the device. See chapter 42 for more information about policies and policy distribution.

Procedure 22-23 To create a static configuration for a SRLG Policy

This procedure describes how to create a static configuration for a SRLG policy. This differs from the standard SRLG policy described in Procedure 22-22 in that it allows you to manually enter into the SRLG database the SRLG membership for links in the entire network. This is typically done at the 7x50 head-end node and is mutually exclusive with the reading of this information from the traffic engineering database.

There are deployments where the 7x50 head-end node interoperates with routers that do not implement the SRLG membership advertisement using IGP SRLG Type-Length Value (TLV) or sub-TLV. In these situations, you can manually enter the link members of SRLG groups for the entire network at any 7x50 node which needs to signal LSP paths, such as a head-end node.

1 Choose Policies→MPLS→Shared Risk Link Group Static Configuration from the 5620 SAM main menu. The Manage Shared Risk Link Group Static Configuration form opens.

2 Click on the Create button.

The Static Configuration for SRLGs Policy (Create) form opens with the General tab displayed.

3 Configure the Displayed Name parameter.



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Apply button to save the policy.

The Static Configuration for SRLGs Policy (Edit) form is refreshed and the tabs become selectable. Table 22-10 describes the tabs that you can choose to configure parameters or view fault information.

Table 22-10 Description of Static Configuration for SRLG Policy form tabs

Tab	Description
General	Displays information on the policy and allows you to prepare the policy for release and distribution.
Local Definitions	Lists Static Configuration for SRLG policies and allows you to manage policy distribution.
Routers	Lists and allows you to manage existing static configuration entries or add new ones.
Faults	List and manage alarms related to the static configuration for SRLGs.

5 Click on the Routers tab.

6 Click on the Create button. The Router for Static Config for SRLG policy (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Router ID
- Administrative State

8 Click on the OK button, and then click OK in the confirmation box that appears. The router(s) you added appears in the list on the Routers tab.

9 If you need to add other routers, repeat steps 6 and 7, otherwise, go to step 10.

10 Select one of the routers and click on the Properties button. The Router for Static Config for SRLG policy (Create) form opens with the General tab displayed.

11 Configure the Administrative State parameter.

12 Click on the Interfaces tab.

13 Configure the Interface Ip Address parameter. You can enter this manually or use the Select button to choose from a list.

14 Configure the Displayed Name parameter.



Note — You can associate the same Interface Ip Address parameter with more than one SRLG.

15 Click on the Apply button and repeat steps 10 to 14 to add other entries, or click OK to close the Static Configuration for SRLGs policy (Create) form.

16 If you clicked on Apply in the previous step, you can click on the Distribute button to manually distribute the Static Configuration for SRLGs policy locally to managed devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to managed devices when they are used by resources on the device. See chapter 42 for more information about policies and policy distribution.

Procedure 22-24 To view network resources

This procedure describes how to view current network resources such as IP addresses, duplicate IP addresses, RDs and RTs, and MAC addresses.

1 Choose Network Resources from the Tools menu. The Network resources form opens with the IP Addresses tab displayed.

2 Select the tab for the particular network resource type you need to query. The choices are:

- IP Addresses
- Virtual Router Duplicate IP Addresses
- Route Distinguishers and Route Targets
- MAC Addresses

The form list is refreshed to display the chosen resources.

3 Customize the search as required. Apply a Boolean operator for any of the items in the list header and then do one of the following:

a Choose a specific item type from the adjacent drop down menu (indicated by a downward-pointing arrow).

b Enter a specific string in the adjacent blank text field.

4 Click on the Search button.

The results of your customized search are displayed.

5 Close the Network Resources form.

Procedure 22-25 To view a routing instance or related object

1 Choose Manage→Networking→Routing Instances from the from the 5620 SAM main menu. The Manage Routing Instances form opens.

2 Choose an object from the Select Object Type drop-down menu.

3 Configure the filter criteria, as required, and click on the Search button.

4 Choose an object and click on the Properties button. The appropriate properties form opens with the General tab displayed.

5 Click on the form tabs to view parameters, faults, statistics, and associated objects.

6 Close the properties form.

7 Close the Manage Routing Instances form.

Procedure 22-26 To view routing policy usage

You can use the 5620 SAM to display a list of NEs currently using global or local versions of certain routing policy types. This ability is supported for the following:

- Routing Policy Statements where export and import policies have been associated with sites running these routing protocols: OSPF (v2 and v3), BGP, RIP, ISIS, LDP (export only)
- Routing Policy Statements where VPRN services have associated VRF export and import policies
- Routing Policy Statements where BGP-AD enabled VPLS sites have associated VSI export and import policies
- Prefix Lists
- Communities
- AS Path
- Damping

For Prefix Lists, Communities, AS Path, and Damping policies, the Policy Usage tab lists the policy statements in which the policy is used.

1 Choose Policies→Routing in the 5620 SAM main menu and select the required policy type from the flyout menu. The Routing Policy management form opens.

2 Click the Search button and choose the required policy from the list, then click Properties. The appropriate Routing Policy (Edit) form opens.

3 Click the Policy Usage tab.

4 If you are examining a Routing Policy Statement, click on the required protocol sub-tab. For LDP, RIP, and BGP you must also click on one of the sub-tab options under these, such as Site, Peer, Peer Groups, Group, or Interface, as appropriate.

5 Choose an entry from the list and click on the Properties button. The properties form for the item opens, with the General tab displayed.

6 Close the properties form.

7 Close the Routing Policy management form.

Procedure 22-27 To view DHCPv6 leases

This procedure describes how to view the DHCPv6 prefixes that the server has given out.

1 Choose Routing from the navigation tree view selector.

2 Navigate to a routing instance by choosing Network→NE→Routing Instance.

3 Right-click on the routing instance icon and choose Properties from the menu. The Routing Instance (Edit) form opens with the General tab displayed.

4 Click on the Local DHCP Servers tab.

5 Click on the Local DHCPv6 tab. The list of associated DHCPv6 servers is displayed.

6 Choose a DHCPv6 server and click on the Properties button. The Local DHCPv6 Server (Edit) form opens with the General tab displayed.

7 Click on the Show Leases button. If the Show Leases button is not visible, click on the More Actions button and choose Show Leases. The Local DHCPv6 Server Show Leases form opens.

8 Perform one of the following:

a To view the entire list of leases that are active on the DHCPv6 server, click OK.

b To view the lease information for a specific prefix, enter the IP address in the Prefix parameter for the particular DHCPv6 server and click OK.



Note — If the prefix does not exist in the list of leases, a message displays.

c To view the detailed lease information for a specific prefix, enter the IP address in the Prefix parameter for the particular DHCPv6 server, select the Detail check box, and click OK. The form displays the CLI details for the specific prefix.

9 Close the Local DHCPv6 Server Show Leases form.

10 Close the Local DHCPv6 Server (Edit) form.

11 Close the Routing Instance (Edit) form.

Procedure 22-28 To view DHCPv6 log events

This procedure describes how to view lease not owner and pool unknown log events for local DHCPv6 servers.

1 Choose Routing from the navigation tree view selector.

2 Navigate to a routing instance by choosing Network→NE→Routing Instance.

3 Right-click on the routing instance icon and choose Properties from the menu. The Routing Instance (Edit) form opens with the General tab displayed.

4 Click on the Local DHCP Servers tab.

5 Click on the Local DHCPv6 tab. The list of associated DHCPv6 servers is displayed.

6 Choose a DHCPv6 server and click on the Properties button. The Local DHCPv6 Server (Edit) form opens with the General tab displayed.

7 Click on the Logs tab. The Lease Not Owner Log and Pool Unknown Log tabs display.

8 Click on the tab for the type of log that you wish to display. Configure the filter criteria and click on the Search button. A list of NE SHCV event logs appears.

9 Configure the filter criteria and click on the Search button. A list of event logs appears.

10 Choose a log entry and click on the Properties button. The Log form opens.

11 View the log entry.

12 Close the Log form.

13 Close the Local DHCPv6 Server (Edit) form.

14 Close the Routing Instance (Edit) form.

Procedure 22-29 To view a routing policy from a CLI session

To view a routing policy from a CLI session, navigate to the previously distributed local routing policy or view navigate to a routing instance by choosing Network→NE→Routing Instance. See Procedure 22-1 for more information.

1 Perform one of the following depending on which routing policy you need to view from a CLI session.

   a Choose Policies→Routing→Statement from the 5620 SAM main menu. A Routing Policy - Statements form opens.

   b Choose Policies→Routing→Prefix List from the 5620 SAM main menu. A Routing Policy - Prefix Lists form opens.

   c Choose Policies→Routing→Community from the 5620 SAM main menu. A Routing Policy _ Communities form opens.

   d Choose Policies→Routing→Damping from the 5620 SAM main menu. A Routing Policy _ Dampings form opens.

   e Choose Policies→Routing→AS Paths from the 5620 SAM main menu. A Routing Policy - AS Paths form opens.

2 Click on the Search button. A list of policies appears.

3 Choose a policy.

4 Click on the Properties button. A *Policy_type* (Edit) form opens.

5 Click on the Local Definitions tab. A window appears displaying a list of NEs to where the policy was distributed.

6 Choose a site.

7 Click on the Properties button. A *Policy_type* Local Policy (Edit) form opens.

8 Click on the Show Policy button. If the Show Policy button is not visible, click on the More Actions button and choose Show Policy. A Routing Policy Show Policy form opens with the General tab displayed.

9 Click on the OK button. A CLI display is initiated.

10 View the policy.

11 Click on the close button.

12 Close the A *Policy_type* Local Policy (Edit) form.

Procedure 22-30 To list MVPN Extranet objects for a NE

Perform this procedure to display a list of MVPN extranet objects that exchange route information through a given NE. The Show MVPN-Extranet menu command issues a show router mvpn-extranet CLI command to the selected NE, and returns a list of subscriber VRF IP addresses. The command can be issued from a base routing instance, or from a VPRN site.

1 Do one of the following:

- **a** To run the Show MVPN-Extranet command from the navigation tree:
  - **i** Choose Routing from the navigation tree view selector.
  - **ii** Navigate to the Routing Instance icon by choosing Network→<source NE>→Routing Instance.
- **b** To run the Show MVPN-Extranet command from a VPRN site:
  - **i** Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.
  - **ii** Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.
  - **iii** Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens.
  - **iv** In the navigation tree on the left side of the form, navigate to the Routing Instance icon.

2 Right-click on the Routing Instance icon and choose Show MVPN-Extranet from the menu. The Show MVPN-Extranet form opens.

3 In the Parameters field, you can type filter arguments for the show router mvpn-extranet CLI command. For example:

- mvpn-extranet [detail] [srcmvpn <*source_service_id*>] [recvmvpn <*reciever_service_id*>]

where
[detail] provides a detailed route table in the command output.
[srcmvpn <*source_service_id*>] filters the output route table to a source VRF, based on the service ID of the source VRF. The variable range is 0 to 4294967295.
[recvmvpn <*reciever_service_id*>] filters the output route table to a destination VRF, based on the service ID of the destination VRF. The variable range is 0 to 4294967295.

4 Click on the OK button. The Show MVPN-Extranet form displays table of MVPN extranet objects.

Procedure 22-31 To display IOM/IMM Label FIB information

Perform this procedure to display FP tunnel table information for a routing instance.

1 Choose Routing from the navigation tree view selector.

2 Navigate to the Routing Instance icon by choosing Network→<source NE>→Routing Instance.

3 Right-click on the Routing Instance icon and choose Show FP Tunnel Table from the menu. The FP RTR Show FP Tunnel Table form appears.

4 Configure the parameters:

- Slot Number
- IP Prefix
- IP Prefix Length

5 Click on the OK button. The FP RTR Show FP Tunnel Table form displays information about BGP, LDP, and RSVP tunnels on the interface.

Procedure 22-32 To display ECMP/LAG hashing of Epipe services

Perform this procedure to monitor the distribution of Epipe service traffic over a LAG and/or ECMP paths into the network. The Show Service Hashing menu command issues a CLI tools dump command to an NE. The CLI command can be issued from a specific LAG on an NE, or from an Epipe service site.

When you issue this command from a LAG, then only the actual number of Epipe services currently using the physical port of the LAG will be displayed.

Alternatively, you can issue this command from an Epipe site that uses a port associated with a LAG. When you specify a range of Epipe Service IDs, the procedure will display information on all the Epipe services within that range that are using the same LAG as their egress port.

This procedure is only applicable to 7750 SR NEs and is not supported for PBB Epipe services.

1 Perform one of the following:

a To run the Show Service Hashing command from a LAG:

i Choose Equipment from the navigation tree view selector.

ii Navigate to the LAG icon by choosing Network→<required NE>→Logical Groups→LAGs→<required LAG>.

iii Right-click on the required LAG icon and choose Show Service Hashing from the menu.

The Epipe LAG Show Service Hashing form opens and displays the total number of Epipe services currently using the physical port of the LAG.

If an error is detected (for example, an invalid login), then error debugging information will be provided.

b To run the Show Service Hashing command from an Epipe site that uses a LAG:

i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

ii Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

iii Select the required Epipe service and click on the Properties button. The Epipe Service (Edit) form opens.

iv In the navigation tree on the left side of the form, navigate to the required Epipe site.

v Right-click on the site icon and choose Show Service Hashing from the menu. The Epipe Service Show Service Hashing form opens.

vi Enter the desired value in the End Service Id field. This is the highest Service ID in a range of up to 1024 service IDs that will be examined. It can have a value of 0 to 2147483650. The Epipe service from which you issued this command has the lowest Service ID in the range of services that will be examined. So if, for example, the Epipe has a Service ID of 100, then Service IDs up to 1124 will be examined.

Entering a value of 0 in the End Service Id field indicates that the Service ID will not be considered. In this case, only the total number of Epipe services currently using the same physical port as the site's LAG will be displayed.

vii Click the OK button.

The Epipe Service Show Service Hashing form opens and displays specific information on all Epipe services currently using the same physical port as the site's LAG.

If an error is detected (for example, an invalid login), then error debugging information will be provided.

2 Click on the Close button. The Show Service Hashing form closes.

22.6 Network domain configuration procedures

Perform these procedures to configure a network domain.

Procedure 22-33 To create a network domain

1 Choose Routing from the navigation tree view selector.

2 Navigate to the network domains icon by choosing Network→NE→Routing Instance→Network Domains.

3 Right-click on the network domains icon and choose Create Network Domain from the menu. The Network Domain (Create) form opens.

4 Enter:

- Domain Name
- Description

5 Click on the OK button. The Domain Network (Create) form closes and a network domain is created in the navigation tree.

Procedure 22-34 To associate a network interface with a network domain

1 Choose Routing from the navigation tree view selector.

2 Choose Network→NE→Routing Instance→Network Domains→domain-userdomain.

3 Click on the Network Interfaces tab and click on Add Network Interface. The Add Network Interface form opens.

4 Click on Search to display all the Network Interfaces. Choose a Network Interface and click on the OK button. The selected Network Interface is displayed on the Network Domain form.

Procedure 22-35 To remove a network interface from a network domain

1 Choose Routing from the navigation tree view selector.

2 Choose Network→NE→Routing Instance→Network Domains→domain-userdomain.

3 Click on the Network Interfaces tab and select the Network Interface that has to be removed from the domain.

4 Click on Remove Network Interface.

5 A Confirm dialog box opens.

Perform one of the following:

a Click on the No button to avoid removing the network interface. The Confirm dialog box closes.

b Click on the Yes button. The network interface is removed from the network domain.

Procedure 22-36 To associate a service tunnel with a network domain

1 Choose Routing from the navigation tree view selector.

2 Choose Network→NE→Routing Instance→Network Domains→domain-userdomain.

3 Click on the Service Tunnels tab and click on Add Tunnel. The Add Tunnel form opens.

4 Click on Search to display all the service tunnels. Choose a service tunnel and click on the OK button. The selected service tunnel is displayed on the Network Domain form.

Procedure 22-37 To remove a service tunnel from a network domain

1 Choose Routing from the navigation tree view selector.

2 Choose Network→NE→Routing Instance→Network Domains→domain-userdomain.

3 Click on the Service Tunnels tab and select the service tunnel that has to be removed from the domain.

4 Click on Remove Tunnel.

5 A Confirm dialog box opens.

Perform one of the following:

a Click on the No button to avoid removing the service tunnel. The Confirm dialog box closes.

b Click on the Yes button. The service tunnel is removed from the network domain.

Procedure 22-38 To delete a network domain

1 Choose Routing from the navigation tree view selector.

2 Navigate to the network domains icon by choosing Network→NE→Routing Instance→Network Domains.

3 Right-click on the network domains icon and choose Delete from the menu. A Confirm dialog box opens.



Caution 1 — The default network domain cannot be deleted.

Caution 2 — The network domain related to the Interface and SDP cannot be deleted.

4 Perform one of the following:

a Click on the No button to avoid deleting the network domain. The Confirm dialog box closes.

b Click on the Yes button. The network domain is deleted from the navigation tree.

23 — Protocol configuration

23.1 Protocol configuration overview ***23-3***

23.2 Workflow to configure protocols ***23-24***

23.3 Workflow to configure BGP ***23-25***

23.4 Workflow to configure RIP ***23-26***

23.5 Workflow to configure LDP ***23-26***

23.6 Workflow to configure IS-IS ***23-26***

23.7 Workflow to configure OSPFv2 and OSPFv3 ***23-27***

23.8 Workflow to configure RSVP ***23-27***

23.9 Workflow to configure L2TP ***23-27***

23.10 Workflow to configure PIM ***23-28***

23.11 Workflow to configure IGMP ***23-28***

23.12 Workflow to configure MSDP ***23-29***

23.13 Workflow to configure MLD ***23-29***

23.14 Workflow to configure bridging on an OmniSwitch device ***23-29***

23.15 Workflow to configure WPP ***23-29***

23.16 BGP configuration procedures ***23-30***

23.17 RIP configuration procedures ***23-49***

23.18 LDP configuration procedures ***23-52***

23.19 IS-IS configuration procedures ***23-64***

23.20 OSPF configuration procedures ***23-75***

23.21 RSVP configuration procedures ***23-87***

23.22 L2TP configuration procedures ***23-90***

23.23 PIM configuration procedures ***23-98***

23.24 IGMP configuration procedures ***23-119***

23.25 MSDP configuration procedures ***23-126***

23.26 MLD configuration procedures ***23-134***

23.27 Bridging configuration procedures ***23-140***

23.28 WPP configuration procedure ***23-148***

23.1 Protocol configuration overview

The 5620 SAM allows you to configure routing protocols and navigate to the device parameters. One device can support multiple routing protocols.

You use the network, IS-IS, and OSPF views in the 5620 SAM GUI navigation tree to view and configure parameters that set and manage the device routing protocol support. The routing protocols are enabled on the devices when you configure the devices. You configure the Layer 3 interfaces when you configure the routing instance on the device. You can then configure the routing protocols for specific Layer 3 interfaces.

Supported routing protocols include:

- IPv6
- BGP
- MP-BGP
- RIP
- LDP
- IS-IS
- OSPF
- RSVP
- L2TP
- PIM
- IGMP
- MSDP
- MLD
- Bridging
- WPP

Routing protocols can be configured to import or export routes from other routing protocols using routing policies. See "Routing policies" in section 22.1 for more information.

In addition to routing protocols, the 5620 SAM supports the following router configurations:

- multicast protocols
  - PIM; see section 23.23 for more information
  - IGMP; see section 23.24 for more information
  - MSDP; see section 23.25 for more information
  - MLD; see section 23.26 for more information
- bridging on OmniSwitch devices; see section 23.27 for more information

For more information about managing routing objects and protocols in the 5620 SAM, see section 22.1.

IPv6 support

The 5620 SAM supports IPv6 for control-plane addressing on IPv6-enabled devices.

Although the implementation of IPv6 is driven by the diminishing IPv4 address space, it is increasingly necessary to use a protocol that is designed to handle more complex network applications, such as broadband voice and video transmission, IP transit, Internet exchange peering, and other large enterprise applications.

Transition from IPv4 to IPv6

The transition from IPv4 to IPv6 is occurring in stages as network providers, service providers, and end users migrate existing applications and equipment to the new version. Control-plane forwarding of IPv6 packets is an important part of this transition; it allows isolated IPv6 hosts and smaller IPv6 networks to peer across an IPv4 network, using a mechanism such as 6over4 tunneling.

With 6over4 tunneling, a host encapsulates IPv6 packets in IPv4 packets for transport across an IPv4 network. Routers that identify 6over4 encapsulation remove the IPv4 encapsulation before they forward the packets to other native IPv6 hosts. The 6over4 mechanism uses the IPv4 multicast infrastructure for neighbor discovery.

IPv6 benefits

The general benefits of IPv6 include:

- **simplified header format and fixed header length**
  An IPv6 header contains fewer fields than an IPv4 header. IPv6 excludes obsolete IPv4 header fields and processes option fields only when they contain values. IPv6 also standardizes the size of the packet header to 40 bytes to streamline packet processing. These features reduce packet-processing overhead and make routing more efficient.
- **addressing enhancements**
  IPv6 increases the IP address size from 32 bits to 128 bits to support a greater number of NEs and to provide a more versatile addressing hierarchy. IPv6 also supports address autoconfiguration.
  The scalability of multicast routing is improved by the presence of a Scope field. IPv6 introduces anycast addressing, which designates a group of disparate NEs as the recipient of a specific data stream.
- **improved scalability and extensibility**
  Built-in traffic optimization makes IPv6 highly scalable, and IPv6 supports future routing technology enhancements using protocol extensions.
- **flow-labeling capability**
  IPv6 features packet prioritization which allows the labeling of packets that require special handling, such as real-time service for VoIP conferences.
- **improved privacy and security**
  Authentication, encryption, and data integrity features are mandatory components for which IPv6 supports standardized extensions.

The 5620 SAM and IPv6

The 5620 SAM entities that support IPv6 configuration include the following:

- BGP for base routing instances and VPRN services
- IS-IS adjacencies
- multicast routing
- static routes
- ICMP
- routing policies
- access ingress and egress policies
- CPM filter policies
- PPP
- IES and VPRN SAPs
- IES and VPRN bidirectional forwarding detection
- VLL Ipipe
- PIM-SSM

A 5620 SAM operator enables IPv6 on an interface during interface creation.

The benefits of the 5620 SAM IPv6 implementation include:

- integration with existing IPv4 configurations on many property and configuration forms
- automatic validation of IP addresses on the client GUI, regardless of the IP version
- support of compressed IPv6 addresses when repeated address octets are present
- support for IPv6 statistics
- simultaneous IPv4 and IPv6 support by routing protocols
- separate IPv4 and IPv6 administrative and operational states on an interface

Accepted IPv6 address formats

The 5620 SAM accepts IPv6 addresses in the following formats:

- colon-hexadecimal, or *x:x:x:x:x:x:x:x*
  where *x* is a 16-bit hexadecimal number from 0 to FFFF
- a combination of colon-hexadecimal and dotted-decimal, or *x:x:x:x:x:x:d.d.d.d*
  where
  x is a 16-bit hexadecimal number from 0 to FFFF
  d is an 8-bit decimal number from 0 to 255

Using a combination of colon-hexadecimal and dotted-decimal formats may be convenient in an environment that supports the use of IPv4 and IPv6 addresses.

The 5620 SAM allows IPv6 address compression for an address that contains repeated zero values. You can use two adjacent colons to represent any group of repeated zero values in an IPv6 address. For example:

2001:DB8::

expands to

2001:0DB8:0000:0000:0000:0000:0000:0000

It is not necessary to supply the leading zeros for a number in an IPv6 address. For example, 2001:DB8::3C:5 is a valid IPv6 address.

BGP

BGP is an inter-AS routing protocol. An AS is a network or a group of devices logically organized and controlled by a common network administration. BGP enables devices to exchange network reachability information. AS paths are the routes to each destination. There are two types of BGP: IBGP and EBGP.

- IBGP is used to communicate with peer devices in the same AS. Routes received from a device in the same AS are not advertised to other devices in the same AS but can be advertised to an EBGP peer.
- EBGP is used to communicate with peers in different ASs. Routes received from a device in a different AS can be advertised to both EBGP and IBGP peers.

See "Inter-AS connections" in section 71.1 for more information about connecting ASs in a VPRN.

You can use the 5620 SAM to enable BGP on the device and perform the following functions:

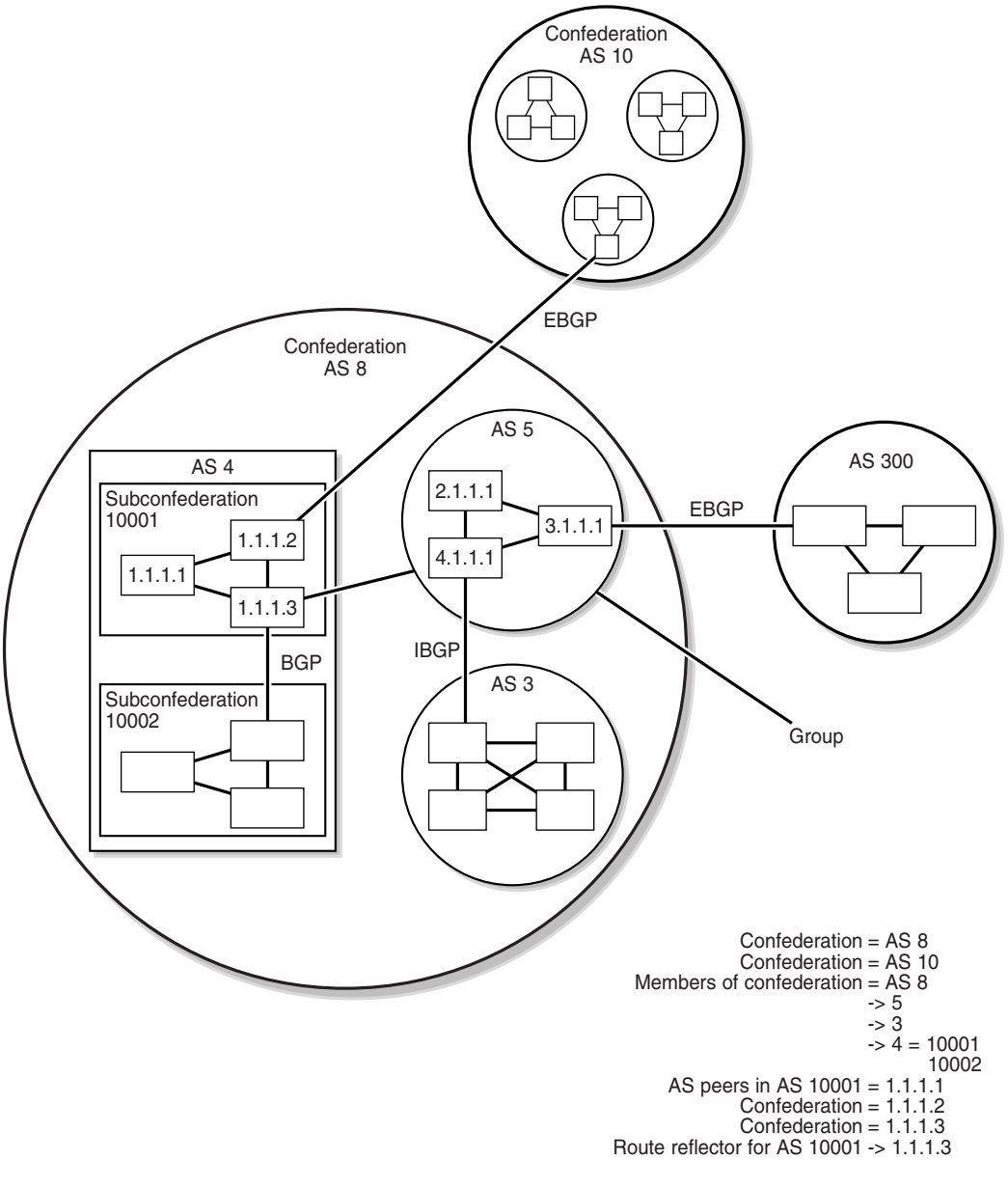
- set the AS values for the routing instance
- create confederations of group-managed devices
- create BGP peer groups
- create neighbors (peers) within the BGP peer groups

The 5620 SAM supports the configuration of IPv6 addresses for BGP peering on the base routing instance of the 7950 XRS, the 7750 SR (chassis modes C and D, and chassis modes A and B with mixed mode enabled), and the 7450 ESS in mixed mode.

A device can only belong to one AS. After the neighbor relationship is established between devices, they exchange BGP open messages, which contain information such as AS numbers, BGP versions, router IDs, hold-time values, and keepalive messages. This information determines the status of the BGP session. Peer relationships are defined by configuring the IP addresses of the devices that are peers of the local BGP system.

Figure 23-1 shows a simple BGP example using groups, subconfederations, and confederations.

Figure 23-1 BGP example



In a standard BGP configuration, all BGP-enabled devices within an AS have a full mesh of BGP peerings to ensure all externally learned routes are redistributed through the entire AS. This is needed because IBGP does not re-advertise routes learned from one IBGP peer to another IBGP peer. However, as more devices are added, scaling the IBGP mesh can become an issue. To solve this scaling issue, you can use:

- confederations
- subconfederations

Confederations are a way to subdivide a large AS into smaller ASs. Subconfederations further subdivide ASs. Within each smaller AS, or confederation, IBGP is still used, however EBGP is used between subconfederations. This means less meshing between peers is required.

Another method of subdividing an AS is route reflection. For route reflection, an AS is divided into groups called clusters. Each cluster contains at least one route reflector. The route reflector redistributes routing updates to all devices in its cluster. Because the route reflector provides all the routing updates, the other devices in the cluster do not maintain a BGP mesh.

By default, BGP routers will advertise only the best path to other BGP peers. When the best path fails or a better path is discovered, the old routing information is overwritten. If BGP Add-Path is enabled, peers will advertise multiple paths for the same destination, all of which will be retained in their routing tables. In the event of a failure or path withdrawal message, the router is able to update its forwarding entry for that destination without having to receive new path advertisements. This results in faster convergence after path failure.

MP-BGP

BGP distributes IP routing information between networks. The distribution of IP routing information between VPRNs requires MP-BGP. MP-BGP addressing uses an 8-byte RD with a 4-byte or 16-byte IP address, depending on whether IPv4 or IPv6 is used. The requirements for MP-BGP configuration are the following.

- MP-BGP must be enabled on the participating PE devices.
- All PE devices must be configured as BGP peers.

When PE devices learn routing information from the CE devices in a VPRN configuration, the routing information is shared using MP-BGP. The RD is used to associate the new routing information with a VPRN instance.

The PE devices distribute the route information to the other CE devices in the VPRN. Each learned route is assigned an MPLS label that is distributed to the devices.

When customer packets arrive at a PE device, the packets are encapsulated with the MPLS label that corresponds to the learned route for the packet destination.

The MP-BGP multicast extension can be applied to build separate routing tables for multicast paths. IGPs such as OSPF and IS-IS can import multicast and unicast routing information to the multicast and unicast routing tables. The multicast routing information can subsequently be used by PIM to perform RPF lookups.

RIP

RIP is an IGP that uses a distance-vector algorithm to determine the best route to a destination, using hop count as the deciding factor. In order for the protocol to provide complete information about routing, every device in the domain must participate in the protocol. RIP, a UDP-based protocol, updates its neighbors, and the neighbors update their neighbors.

Unlike OSPF and other link-state protocols, RIP directly advertises reachability information to its neighbors. RIP advertises reachability information by sending prefix, mask, and either hop count or cost metric data. Each device running the RIP protocol advertises all RIP devices periodically by sending RIP update PDUs. The route with the lowest metric is advertised as the best route.

The 5620 SAM supports the configuration of RIPv1 and RIPv2 on network and access interfaces.

The 5620 SAM supports the configuration of IPv6 addresses for RIP on the base routing instance of the 7750 SR (chassis modes C and D, and chassis modes A and B with mixed mode enabled).

LDP

LDP is used to distribute labels in non-traffic-engineered MPLS applications. Routers can establish LSPs across a network by mapping network-layer routing information directly to the data link layer switched paths. After the LDP distributes the labels to the LSR, the LSR assigns the label to a FEC, and then informs all other LSRs in the path about the label and how the label switches data accordingly.

A FEC is a collection of common actions associated with a class of packets. LDP helps establish the LSP by providing a set of procedures that LSRs can use to distribute labels.

When a service tunnel is configured on managed routers using LDP signaling in an MPLS environment, LDP sessions are set up based on the configured hello and other PDU values. If another service tunnel is created to the same destination, the LDP session is reused.

The LDP sessions between LSRs:

- find and establish LDP peers in the managed network
- exchange label mappings for each LSR
- exchange label bindings

After all the LSRs are LDP-aware and the LSP is created, forwarding can occur as follows:

1 A FEC is associated with the LSP.

2 The FEC maps the packets to the LSP.

3 The next LSR that is part of the LSP splices incoming FEC labels to the outgoing FEC label of the next hop.

There are two types of LDP:

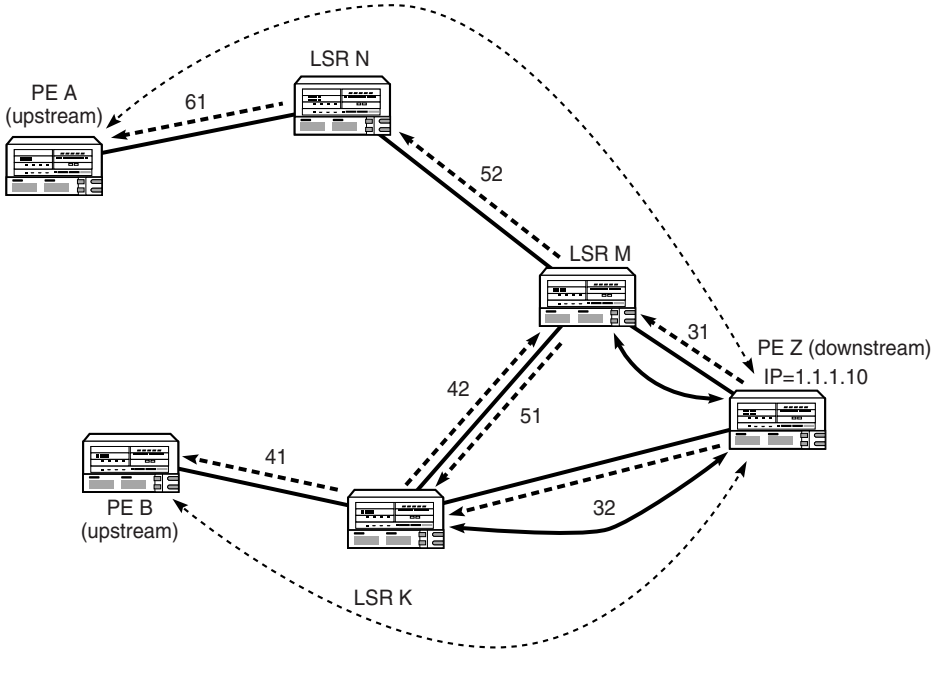
- T-LDP
- DU-LDP

T-LDP is used to distribute labels for VLL and VPLS. T-LDP allows the targeting of remote devices that are not directly connected as targeted peers.

DU-LDP can be used to create tunnels between PEs for IP-VPN services.

Figure 23-2 shows an example of LDPs that are used in a simple Layer 2 and Layer 3 service provider network.

Figure 23-2 LDP sample network



- The solid straight lines between the devices indicate IP connectivity. These are directly connected peers.
- The dotted bidirectional curved lines indicate T-LDP sessions. These are targeted peers that are not directly connected.
- The solid bidirectional curved lines indicate DU-LDP sessions. This example only shows two instances, between M and Z, and Z and K. If there is IP connectivity between all the devices, then all of the devices have DU-LDP sessions.

Provider edge router Z advertises the labels for its address 1.1.1.10 to adjacent link state devices M and K. Routers M and K distribute the labels for that address to the rest of the network.

If provider edge router A wants to send a VPN-labeled packet to router Z, it uses label 61 as the outer label. When the packet reaches router N, outer label 61 is swapped for outer label 52 and the packet continues downstream to router M. Router M then swaps out label 52 for either outer label 31 or 42, depending on the router M label selection algorithm. If outer label 31 is selected, the packet reaches router Z directly, which then continues to route the packet to the customer site based on the VPN label.

If a router receives more than one request for an IP address, and the router does not support ECMP, it selects the first label it receives. If the router supports ECMP, it selects the label with the lowest cost path, or selects both labels if the cost paths are identical.

When a router supports ECMP protocol, LSRs can have multiple equal cost paths to an IP address. ECMP LDP retains all labels it receives from multiple next hop peers. The forwarding plane contains multiple next hops for a FEC and as a result, provides load balancing for LDP-based LSPs.

When a router supports ECMP LDP and a device configured as the next hop is no longer valid, for example a session between peers is lost or the peer withdraws its label, a new valid LDP next hop peer is selected and the forwarding plane is updated.

Load balancing across LSPs for LDP over RSVP is also supported. When ECMP is enabled, all equal cost LSP endpoints are installed in the routing table by the IGP for consideration by LDP. LDP selects the LSP with the lowest LSP metric to determine the next hop. If multiple LSPs are available with equal cost, then ECMP is utilized until the ECMP count is exhausted. An LDP tree is created by sending LSP Trace messages along an ECMP path to downstream LSR NEs.

LDP for P2MP

LDP support for P2MP can be enabled on an LDP interface. You can configure an LDP interface for multicast traffic forwarding towards a downstream NE. LDP configuration allows an exchange of P2MP FEC via an established session to a peer, and the use of next hops over an interface.

LDP configuration is supported on a tunnel interface under a base routing instance and under protocols such as PIM and IGMP. A P2MP ID is used as an index for LDP-based tunneling instead of an LSP ID.



Note — BFD and source redundancy are only supported on an RSVP tunnel interface.

IS-IS

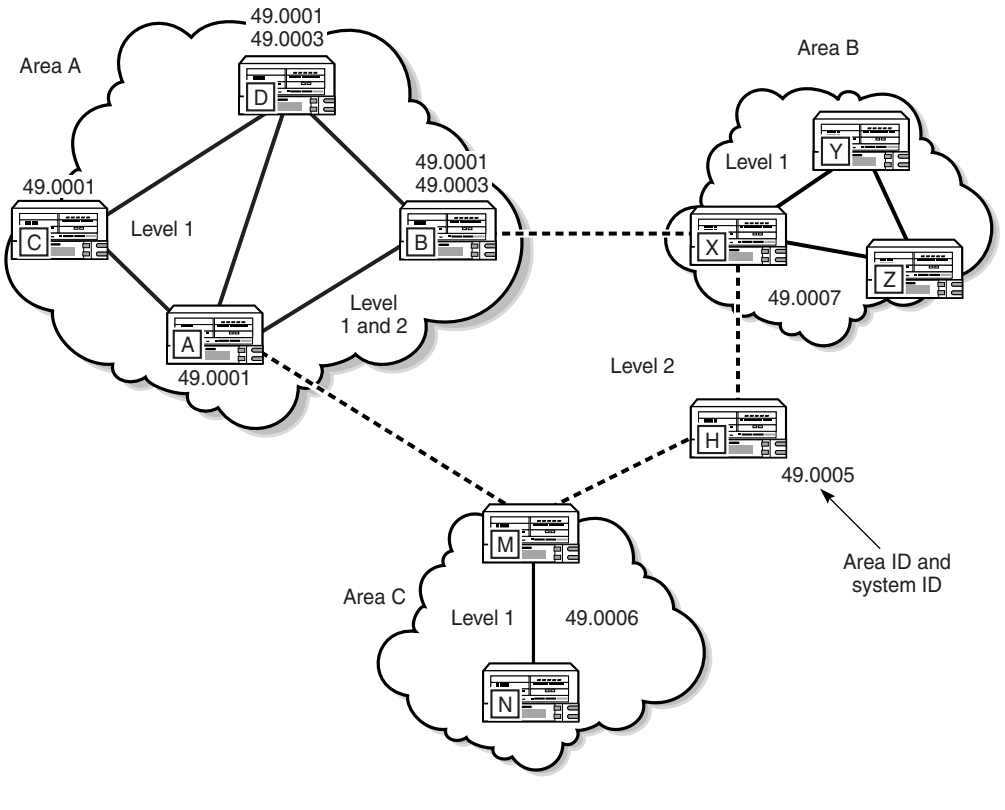
IS-IS is a link-state interior gateway protocol that uses the shortest path first algorithm to determine a route. Routing decisions are made using the link-state information. IS-IS entities include:

- networks, which are autonomous system routing domains
- intermediate systems, which are routers
- end systems, which are network devices that send and receive PDUs

End systems and intermediate system protocols allow devices and NEs to identify each other. The IS-IS protocol sends link state updates periodically through the network, so each device can maintain current network topology information.

Large networks, or autonomous systems, are supported by IS-IS using a two-level hierarchy. This divides a large area into more manageable, smaller areas. The first level (level 1) of routing is performed within an area. The second level (level 2) of routing is performed between areas, as shown in Figure 23-3.

Figure 23-3 IS-IS routing domains example



Level 2 areas are also called backbones, similar to an OSPF backbone area. All traffic traversing different areas must traverse the backbone. A device can be configured as level 1, level 2, or both level 1 and 2. In this example, routers A, B, M, H, and X form the level 2 IS-IS backbone. The connection between routers A and B carries both level 1 and level 2 link-state PDUs (LSPs). However, level 1 devices are only aware of their own area's topology, and must forward traffic to a level 1/2 device to forward the data to another area.

Two devices are in the same level 1 area when they have level 1 adjacency. Level 1 adjacency occurs when the area IDs are common and there is a level 1 connection between the devices. Level 2 adjacency occurs when it has at least one level 1 and 2, or one level 2 interface configured.

The 5620 SAM supports the configuration of IPv6 addresses for IS-IS adjacencies.

Note — If two neighboring devices in the same level 1 area run both level 1 and 2, they establish both a level 1 and a level 2 adjacency.

When LDP over RSVP is enabled for IS-IS, LSPs can be used by the IGP to calculate its SPF tree. The IGP then provides LDP with all of the ECMP IDP next-hops and tunnel endpoints that the IGP identifies as the lowest cost path to the destination. If an IGP calculation and an LDP over RSVP have the same cost, LDP chooses an LDP over RSVP tunnel over an IGP route and ECMP between the two types is not considered. The type and number of tunnels that are to be considered by LDP depend on the IGP costs, where the lowest cost between the tunnel endpoint and the target is selected.

After IS-IS is configured, routing occurs as follows:

1 Hello PDUs are sent to IS-IS-enabled interfaces to discover neighbors and establish adjacencies.

2 IS-IS neighbor relationships are formed.

3 Link-state PDUs (LSPs) are created based on local interfaces and prefixes that are learned from adjacent devices.

4 The devices flood LSPs to adjacent neighbors, and build a link-state database.

5 A shortest path tree is calculated by the IS-IS and the routing table is built.

OSPF

OSPF is a hierarchical link-state interior gateway protocol that operates within ASs and is used in IP networks. OSPF packets are routed based on the destination IP address of the IP packets. Each OSPF router collects link-state information to build a network topology based on OSPF areas. This topology is used to apply the Dijkstra algorithm to calculate the shortest path to each destination in the network. See the appropriate device documentation for more information about OSPF.

When LDP over RSVP is enabled for OSPF, LSP can be used by the IGP to calculate its SPF tree. The IGP then provides LDP with all of the ECMP IDP next-hops and tunnel endpoints that the IGP identifies as the lowest cost path to the destination. If an IGP calculation and an LDP over RSVP have the same cost, LDP chooses an LDP over RSVP tunnel over an IGP route and ECMP between the two types is not considered. The type and number of tunnels that are to be considered by LDP depend on the IGP costs, where the lowest cost between the tunnel endpoint and the target is selected.

OSPF areas

The hierarchical design of OSPF allows a collection of networks to be grouped into a logical OSPF area. The topology of the area is hidden from the rest of the AS, which significantly reduces OSPF protocol traffic. Routing in the AS takes place on two levels, depending on whether the source and destination of a packet reside in the same area (intra-area routing) or different areas (inter-area routing). In intra-area routing, the packet is routed solely on information obtained within the area; routing information obtained from outside the area is not used. Routers that belong to more than one area called an ABR. An ABR maintains a separate topological database for each area it is connected to. Every router that belongs to the same area has an identical topological database for that area.

OSPF neighbor

Routers in the same broadcast domain or at each end of a point-to-point telecommunications link form adjacencies when they detect each other. The detection occurs when a router identifies itself in a hello OSPF protocol packet. This is called a two-way state and is the most basic relationship. The routers in an Ethernet or frame relay network select a designated router and a backup designated router which act as a hub to reduce traffic between routers. OSPF uses both unicast and multicast to send hello packets and link state updates.

The OSPF protocol establishes and maintains neighbor relationships in order to exchange routing updates with other routers. The neighbor relationship table is called an adjacency database in OSPF. Provided that OSPF is configured correctly, OSPF forms neighbor relationships only with the routers directly connected to it. In order to form a neighbor relationship between two routers, the interfaces used to form the relationship must be in the same area. An interface can only belong to a single area.

OSPF super-backbone

The OSPF super-backbone provides an additional layer of hierarchy in OSPF. The OSPF super-backbone functions include:

- loop prevention
- handling LSAs received from the CE
- managing VPN IPv4 routes received by BGP

The PE routers that connect OSPF areas to the super-backbone function as ABRs in the OSPF areas to which they are attached. To achieve full compatibility, the PE routers can also serve as ASBRs in non-stub areas.

PE routers insert inter-area routes from other areas into the area in which the CE router is present. The CE routers are not involved at any level and are not aware of the super-backbone or other OSPF areas that exist outside of the super-backbone.

When you configure the super-backbone, all destinations that are learned by PEs with matching domain IDs become inter-area routes.

See the appropriate device documentation for more information about the OSPF super-backbone.

RSVP

RSVP is a network control protocol that hosts use to request specific qualities of service from the network for specific data streams. RSVP is also used to deliver QoS requests to all devices in a data path and to establish and maintain the state information required to provide the requested service quality.

RSVP is not a routing protocol. RSVP operates using unicast and multicast routing protocols. RSVP consults local routing tables to relay RSVP messages. By default, RSVP is enabled on all devices that support it.

RSVP requests typically result in the reservation of resources on each device in the data path. MPLS uses this RSVP mechanism to set up traffic-engineered LSPs. RSVP requests resources for unidirectional flows only. RSVP treats a sender as logically distinct from a receiver, although the same application process may act as both a sender and a receiver.

The RSVP hello protocol detects the loss of a neighbor NE or the reset of a neighbor RSVP state information. In standard RSVP, neighbor monitoring occurs as part of the RSVP soft-state model. The reservation state is maintained as cached information that is first installed and then periodically refreshed by the ingress and egress LSRs.

If the state is not refreshed within a specified time interval, the LSR discards the state because it assumes that either the neighbor NE has been lost or its RSVP state information has been reset.

Diff-Serv Traffic Engineering support

The 5620 SAM supports Diff-Serv Traffic Engineering, or TE, extensions for RSVP. Diff-Serv TE extensions provide the ability to manage bandwidth in an MPLS network on a per-TE-class basis. With Diff-Serv TE, an LER can perform this on a per-class basis. Therefore, you can set different limits for admission control of LSPs in each TE class over each link in the network.

You do this by setting a bandwidth constraint, which configures the percentage of the RSVP interface bandwidth that each CT shares. The absolute value of the CT share of the interface bandwidth is derived as the percentage of the bandwidth advertised by IGP in the Maximum Reservable link bandwidth TE parameter, that is, the link bandwidth multiplied by the RSVP interface subscription parameter.

This configuration also exists at the RSVP interface level and the value specifically configured for the interface overrides the globally-configured value. The bandwidth constraint value can be changed on the fly. You are also allowed to specify the bandwidth constraint for a CT which is not used in any of the TE class definitions and which is not used by any LSP originating or transiting this NE.

To enable this feature, in summary, you must:

- configure Diff-Serv Classes on the router RSVP Routing Instances
- configure protocol properties to allow Diff-Serv Classes on the required router RSVP Interfaces
- configure traffic engineering and specify the Class Type that the required dynamic LSPs belongs to
- configure the Diff-Serv Class Type that the required LSP Paths belongs to. This overrides the value set at the LSP level.
- configure Diff-Serv to LSP FC mappings on the required service tunnels (SDPs). User-entered mappings of FC to LSP name are validated automatically (to avoid configuration conflicts) by checking with the RSVP module.

L2TP

L2TP is a session-layer protocol that extends the PPP model by allowing L2 and PPP endpoints to reside on different devices that are interconnected by a PSN. L2TP extends the PPP sessions between the CPE and PPP/L2TP termination point on the L2TP network server (LNS), via an intermediate L2TP access concentrator (LAC). The LAC is the initiator of session-generated L2TP tunnels; the LNS is the server that waits for new tunnels. Manually configured and initiated L2TP tunnels can be initiated and stopped from either the LNS or LAC.

After an L2TP tunnel is established, the network traffic between the peers is bidirectional. If a tunnel carrying a session fails, another tunnel from the same tunnel group re-establishes the session. Within each L2TP tunnel, one or more L2TP sessions can exist. Each L2TP session transports PPP packets.

The 5620 SAM supports the configuration and management of the following:

- ISA-LNS groups
- L2TP sites
- L2TP tunnel group profiles
- L2TP tunnel profiles

ISA-LNS groups

The 5620 SAM supports the creation and configuration of ISA-LNS groups on the 7750 SR. ISA-LNS groups provide LNS PPP session termination. An ISA-LNS group is associated with specific L2TP inbound peers and groups. Session traffic is automatically balanced across the available active ISA broadband application MDAs in the group.

The following operations can be performed on an ISA-LNS group member:

- drain MDA—prevents new sessions from being accepted
- stop drain—allows new sessions to be established
- stop MDA sessions—terminates the active sessions

See Procedure 14-6 for information about creating and configuring an ISA-LNS group.

L2TP sites

By default, L2TP is enabled on a base routing instance, and an L2TP site is created. An L2TP icon appears in the routing view of the navigation tree. An L2TP site does not exist by default on the base routing instance of a 7450 ESS in non-mixed mode.

Certain LAC parameter values can be configured on an L2TP site which can, in turn, be inherited by any child L2TP tunnel group profiles of the site. The Tunnel Session Limit parameter value can only be inherited by an L2TP tunnel group profile.

A tunnel selection blacklist function provides a means to temporarily suspend (or blacklist) tunnels that return one or more specified return codes, indicating that the tunnel is inoperative. The user can specify the manner in which blacklisted tunnels are handled:

- how many tunnels can be blacklisted at any given time
- how long a tunnel can remain blacklisted
- action taken on a blacklisted tunnel when the maximum blacklist period expires

See Procedure 23-34 for information about managing L2TP sites.

L2TP is not enabled by default on a VPRN site. To enable L2TP on a VPRN site, see Procedure 71-3.

L2TP tunnel group profiles

An L2TP tunnel group profile represents the configuration for a group of L2TP tunnels. L2TP tunnel group profiles must be configured on the LNS NE. If a local user database is used on the LAC for session authentication, an L2TP tunnel group profile must be configured on the LAC. When you create an L2TP tunnel group profile, you can configure certain LAC parameter values to be inherited from the parent L2TP site. In turn, the profile can be used by its child L2TP tunnel profile to inherit certain parameter values. The inherited parameter values are used as the default values during L2TP tunnel profile configuration.

The following operations can be performed on an L2TP tunnel group profile that has a configured L2TP tunnel profile:

- drain—prevents new sessions from being accepted
- stop drain—allows new sessions to be established
- stop—closes tunnel instances and terminates the active sessions

See Procedure 23-34 for information about managing L2TP tunnel group profiles.

L2TP tunnel profiles

You can create and manage L2TP tunnel profiles from the Tunnel Group Profile properties form. When you create an L2TP tunnel profile, you can configure certain LAC parameter values to be inherited from the parent L2TP tunnel group profile and L2TP site.

The following operations can be performed on an L2TP tunnel profile:

- start instance—attempts to create new tunnels
- stop instance—attempts to close the tunnels
- drain—prevents new sessions from being accepted
- stop drain—accepts new sessions

See Procedure 23-34 for information about managing L2TP tunnel profiles.

L2TP tunnel instance endpoints

The endpoints of an operational L2TP tunnel are represented by tunnel instance endpoints. You can view tunnel instance endpoints from the Tunnel Instance Endpoints tab on the L2TP Site (Edit) form, and from the Tunnel Group Profile or Tunnel Profile properties form if the endpoint is created using the profile configuration.

An L2TP tunnel instance endpoint is automatically created when:

- a start operation is performed on an L2TP tunnel profile
- an incoming L2TP session is established using group and tunnel profiles
- RADIUS authentication returns a configuration for the tunnel when an incoming L2TP session is authenticated and PPP session authentication determines that L2TP is used, at which point an L2TP session is established.

The following operations can be performed on an L2TP tunnel instance endpoint:

- drain—prevents new sessions from being accepted
- stop drain—allows new sessions to be established
- stop—closes the tunnel instances and terminates the active sessions

See Procedure 23-36 for information about viewing L2TP tunnel instance endpoints.

L2TP peers

An L2TP site can have none or multiple L2TP peers. L2TP peer information is available on the Peers tab of the L2TP Site form. Information about L2TP tunnels for a specific L2TP peer is available on the Tunnels tab of the L2TP Peer properties form.

The following operations can be performed on an L2TP peer:

- drain—prevents new sessions from being accepted
- stop drain—accepts new sessions

L2TP tunnels and tunnel endpoints

You can view information about L2TP tunnels and tunnel endpoints from the L2TP Tunnel - Endpoint A - Endpoint B form. See Procedure 23-35 for information about viewing L2TP tunnels and tunnel endpoints.

L2TP sessions

You can view information about L2TP sessions from the L2TP Session (View) form. You can access the form from the following places in the GUI:

- Manage Residential Subscribers form
- Sessions tab on the L2TP Site (Edit) form
- Sessions tab on the L2TP Tunnel Instance Endpoint (View) form
- L2TP panel on the PPPoE Session form (LAC only)
- L2TP Session button on the Subscriber Host form (LAC only)

See Procedure 23-37 for information about viewing L2TP sessions from the Manage Residential Subscribers form.

PPP sessions

You can view information about PPP sessions from the PPP Session, PPPoE Session, and PPPoA Session forms. You can access the forms from the following places in the GUI:

- Manage Residential Subscribers form
- LNS PPP panel in the L2TP Session (View) form (LNS only)
- PPP Session button in the Subscriber Host form

See Procedure 23-38 for information about viewing PPP sessions.

PIM

PIM is a component of multicast routing that defines the one-to-many or many-to-many transmission of information. You can use the following variations for PIM configurations:

- sparse mode
- dense mode
- source-specific multicast
- bidirectional

Sparse mode is the most common PIM configuration. Sparse mode is used for data transmission to NEs in multiple Internet domains that contain a small ratio of NEs that subscribe to the multicast traffic. Dense mode is used when a large ratio of the potential NEs subscribe to the multicast traffic. In source-specific multicast, paths originate at a single, defined source. Bidirectional PIM is not source-specific.

Anycast RP

Anycast RP for PIM-SM enables fast convergence when a PIM RP router fails. The receivers and sources rendezvous at the closest RP after the router failure. Anycast RP allows an arbitrary number of RPs for each group in a single, shared-tree PIM-SM domain. Triple play configurations that distribute multicast traffic using PIM-SM realize the benefits of fast RP convergence, which helps to avoid the loss of multicast data streams or IPTV delivery to the end user.

Anycast RP for PIM-SM environments is supported in the base routing PIM-SM instance of the service router. The 7950 XRS, 7750 SR, 7710 SR, and the 7450 ESS in mixed mode support Anycast RP in VPRN instances that are configured with PIM.

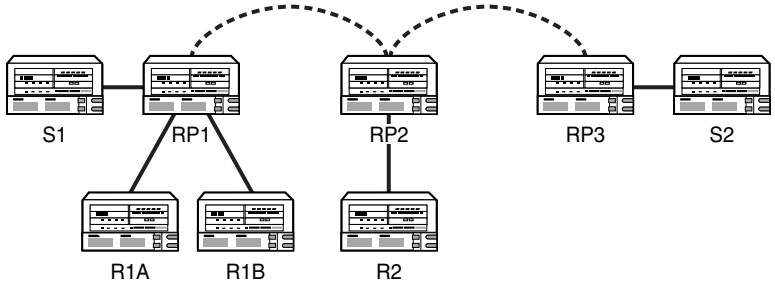
Anycast RP for PIM requires the completion of the following configuration information:

- An IP address specified as the RP address. This address is statically configured, or distributed using a dynamic protocol, to all PIM routers in the domain.
- A set of routers in the domain designated as RPs for the RP address. These routers form an anycast RP.

- Each of these routers is configured with a loopback interface that uses the RP address. The RP address, or a prefix that includes the RP address, is injected into the unicast routing system inside the domain.
- Each router in the anycast RP also needs a separate IP address, to be used for communication between the RPs.
- Each router in the anycast RP is configured with the addresses of all other routers in the anycast RP. The addresses must be consistently configured in all RPs in the set.

Figure 23-4 shows a sample implementation of anycast RP for PIM-SM.

Figure 23-4 Sample implementation of anycast RP for PIM-SM



R1A, R1B, and R2 are receivers for an AnyCast RP group
S1 and S2 send traffic to the AnyCast RP group
RP1, RP2, and RP3 use the same Anycast RP IP address

18605

Table 23-1 summarizes the sequence of events for the Anycast RP implementation shown in Figure 23-4.

Table 23-1 Sequence of events for Anycast RP fast convergence

Sequence	Event description
1	S1 sends a multicast packet.
2	The router connected to S1 forms a PIM registration message to send to the Anycast RP address. The unicast routing system delivers the PIM registration message to the nearest RP, in this case RP1.
3	RP1 receives the PIM registration message, decapsulates the message, and sends the packet down the shared tree to the R1A and R1B receivers.
4	RP1 is configured with the IP address for RP2 and RP3. Since the registration message did not come from one of the RPs in the anycast RP set, RP1 assumes that the packet came from a designated router.
5	RP1 sends a copy of the registration message from the S1 designated router to RP2 and RP3. RP1 uses its IP address as the source address for the PIM registration message.
6	RP1 can join the source tree by sending a join message to S1. However, RP1 must create a source-specific state.
7	RP2 receives the registration message from RP1, decapsulates the message, and send the packet down the share tree to the R2 receiver.

(1 of 2)

Sequence	Event description
8	RP2 sends a registration-stop message back to RP1. RP2 can wait to send the registration-stop message if it decides to join the source tree. RP2 should wait until it receives data from the source tree before it sends the registration-stop message. If RP2 does wait for the data, the registration-stop message is sent to RP1 when it receives the next registration message. If RP2 does not wait for the data, the registration-stop message is immediately sent to RP1.
9	RP2 can join the source tree by sending a join message to S1. However, RP2 must create a source-specific state.
10	RP3 receives the registration message from RP1 and decapsulates the message. No receivers joined for the group, so RP3 discards the packet.
11	RP3 sends a registration-stop message back to RP1.
12	RP3 creates a source-specific state, so when a receiver joins after S1 starts sending traffic, RP3 can quickly join the source tree for S1.
13	RP1 processes the registration-stop message from RP2 and RP3. RP1 can cache the receipt of registration-stop messages from the RPs in the anycast RP set. (The cache of messages is completed on a per-RP or per-source-specific basis.) The cache of messages increases the reliability of the delivery of registration messages to each RP. Subsequent registration messages received by RP1 are sent only to the RPs in the anycast RP set that have not previously sent registration-stop messages from the source-specific entry.
14	RP1 sends a registration-stop message to the DR under the following conditions: • after receiving a registration message from the DR • if all RPs in the anycast RP set have returned registration-stop messages for a specific source-specific route

(2 of 2)

SPT switchover thresholds

SPT switchover thresholds allow you to configure the switchover threshold, in Kbps, for the group prefixes. The threshold value determines when the router switches from the shared tree to the source-specific tree. The switchover is attempted only if the traffic rate on the shared tree for the group exceeds the configured threshold.

L3 Multicast Load Balancing for ECMP

The 5620 SAM distributes multicast traffic by balancing the load based on the total available multicast bandwidth on all ECMP paths. You can configure ECMP rebalancing on the VPRN and base PIM Routing Instance configuration forms.

5620 SAM ECMP rebalancing has the following important characteristics:

- Multicast load balancing over ECMP links is enabled, by default.
- The rebalancing timer is set to 30 minutes, by default.
- Distribution of the multicast groups over the available links is processed based on the bandwidth configured for the specified group address. If the bandwidth is not configured for the multicast stream, then the configured default value is used.
- If a link failure occurs, the load on the failed channel is distributed to the remaining channels. The bandwidth required to accommodate the load from the failed link is evenly distributed over the remaining links.
- If an additional link becomes available for a specific multicast channel, it is then treated in an equivalent manner to the other links of the interface.

- A manual (operator-initiated) rebalance command is typically used to re-evaluate the current balance, with regard to bandwidth utilization. If necessary, multicast streams can subsequently be moved to different links to achieve a balance.
- In an automatic timed rebalance, the system rebalances multicast streams over the available links, based on the configured bandwidth and interval. If no links have been added or removed, or it is determined that no multicast streams will benefit from a rebalance, then it is not be implemented.
- When multicast load rebalancing is not enabled, any ECMP changes are not optimized. However, whenever a link is added, an attempt is made to balance the number of multicast streams on all the available ECMP links. This may however, not result in balanced bandwidth utilization of all the ECMP links.
- Only a single rebalance command can be executed at any specific time. If a rebalance is in progress and a manual rebalance command is entered, it is rejected and a message is displayed informing the user who a rebalance is already in progress.

IGMP

IGMP is a multicast protocol which service providers can use to establish multicast group memberships on a LAN. Within the LAN, end users use IGMP to communicate with a local multicast router, which then uses PIM to distribute the IGMP messages to other local and remote multicast routers. Multicast routers send regular membership queries to IGMP hosts which respond with membership reports. Multicast routers can use these reports to determine which hosts are interested in receiving particular multicast messages.

Configuring a group interface query source IP address on the IGMP site allows a VPLS IGMP snooping instance to register the port facing an ESM port as a multicast router port.

IGMP operates above the network layer on IPv4 networks.

MSDP

MSDP is a protocol that enables multiple PIM-SM domains to communicate with each other using their own RPs. MSDP also enables multiple RPs in a single PIM-SM domain to establish MSDP mesh-groups and to synchronize information between anycast RPs about the active sources being served by each anycast RP peer. The 7950 XRS, 7750 SR, 7710 SR, and the 7450 ESS in mixed mode support MSDP.

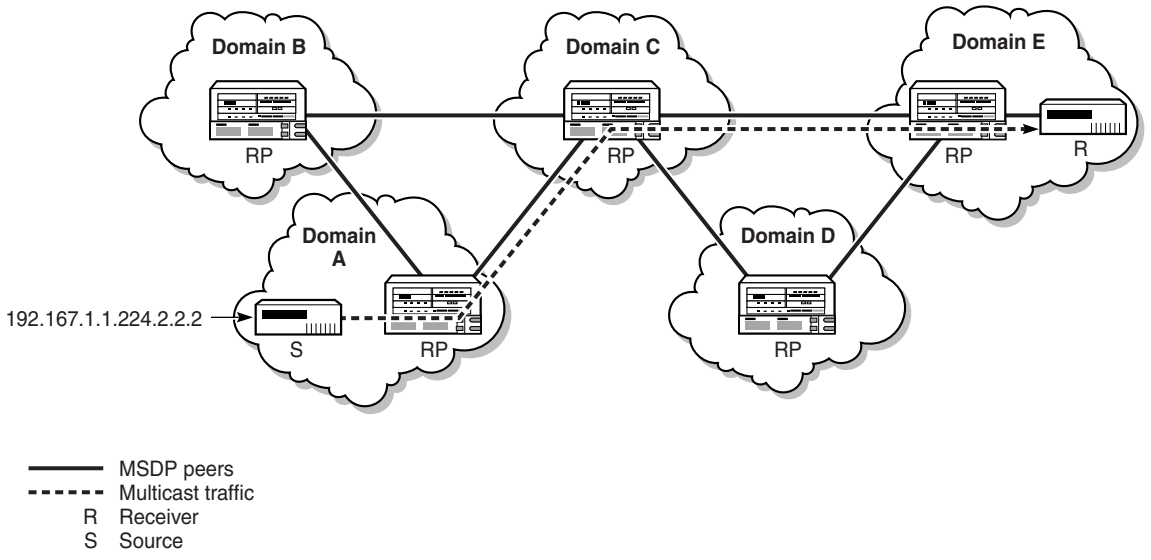
Each PIM-SM domain has its own RPs and MSDP enables these RPs to inform each other about active sources. When an active source is detected, the RPs send PIM-SM explicit join messages to the active source. When RPs in remote domains know about active sources, they can pass on this information to their local receivers and multicast data can be forwarded between the domains.

The RP learns about a new multicast source within its domain through the PIM register mechanism and encapsulates the first data packet in a source active message. After an RPF check, the MSDP source active message is flooded by each peer to its MSDP peers until it reaches every MSDP router in the interconnected networks. If the receiving MSDP peer is an RP, and the RP has a (*,G) entry for the group in the source active message, the message is accepted. The RP creates an (S,G) state for the source and join to the shortest path tree for the state of the source.

The encapsulated data is forwarded down the RP shared tree. When the packet is received by a receiver's last hop router, the last-hop may also join the shortest path tree to the source.

Figure 23-5 shows a sample of how data flows from a source in Domain A to a receiver in Domain E in an MSDP implementation for PIM-SM.

Figure 23-5 Sample implementation of MSDP for PIM-SM



MLD

MLD is an asymmetric protocol used by IPv6 routers to discover the presence of multicast listeners, that is, NEs that wish to receive multicast packets. MLD specifies separate behaviors for multicast address listeners and multicast routers.

The purpose of MLD is to enable each multicast router to discover, for each of its directly attached links, which multicast addresses and which sources have interested listeners on that link. The information gathered by MLD is provided to whichever multicast routing protocol is used by the router, such as PIM, to ensure that multicast packets are delivered to all links where there are listeners interested in such packets.

MLD is supported on the 7950 XRS, in chassis mode C or D, and on the 7750 SR in chassis mode A or B with mixed mode enabled. MLD is supported on all variants of the 7705 SAR.

Bridging

Bridging is used between an OmniSwitch device and a 7450 ESS to create a fast ring. The fast ring bridges the end-user devices, such as BTV set-top boxes, and Layer 2 services, such as VPLS, that distribute multicast traffic. If required, you can configure the devices with MSTP or another STP.

STP is active by default on an OmniSwitch. The default mode of operation is 1x1 mode using RSTP. A loop-free network topology is automatically calculated based on default STP switch, bridge, and port parameter values.

Additional OmniSwitch configuration such as enabling and configuring OmniSwitch learned port security parameters for VLAN ports, DHCP relay, and DHCP snooping can be done while configuring other bridge parameters.

You can configure MVRP as part of the bridging configuration on the OmniSwitch. MVRP provides a mechanism to maintain the contents of dynamic VLAN registration entries for each VLAN, and to propagate that information to other bridges.

In the 5620 SAM, a bridge is represented in the network view below a device, similar to the routing instance of a device.

WPP

WPP (Web Portal Protocol) runs between a BNG and a Web portal server. It is used for Web portal authentication of WLAN users (DHCP hosts). WPP can be enabled on base routing instances or VPRN routing instances.

23.2 Workflow to configure protocols

This workflow assumes the following:

- You know the 32-bit unique router ID prior to configuring OSPF or BGP.
- An AS number is assigned to the device prior to configuring BGP.

1 Enable the routing protocols to be supported on the devices. See the appropriate device documentation for more information. The options are:

- LDP
- IS-IS
- MPLS
- RSVP (enabled by default)
- BGP
- RIP
- L2TP (enabled by default)
- OSPFv2
- OSPFv3
- PIM
- IGMP
- MSDP
- MLD



Note — L2TP is enabled by default on a base routing instance, but not on a VPRN routing instance.

2 Ensure the parameters to implement routing protocols on the Layer 3 interfaces are configured. See chapter 22 for more information.

3 As required on the selected routing protocol, configure routing policies. See chapter 22 for more information.

4 Review the appropriate workflow to configure a routing protocol:

- **a** BGP; see section 23.3 for more information
- **b** RIP; see section 23.4 for more information
- **c** LDP; see section 23.5 for more information
- **d** IS-IS; see section 23.6 for more information
- **e** OSPFv2 or OSPFv3; see section 23.7 for more information
- **f** RSVP; see section 23.8 for more information
- **g** L2TP; see section 23.9 for more information
- **h** PIM; see section 23.10 for more information
- **i** IGMP; see section 23.11 for more information
- **j** MSDP; see section 23.12 for more information
- **k** MLD; see section 23.13 for more information
- **l** bridging; see section 23.14 for more information
- **m** WPP; see section 23.15 for more information

5 As required, configure the protocol for the remote device.

23.3 Workflow to configure BGP

1 Enable BGP on the routing instance. See Procedure 23-1 for more information.

2 Determine whether BGP confederations are necessary. If BGP confederations are necessary:

- **a** Configure the Confederation Autonomous System number on the Routing tab of the Routing Instance configuration form.
- **b** Configure BGP confederation members from the BGP Confederations tab of the Routing Instance configuration form. See Procedure 23-3 for more information.

3 If you are configuring MP-BGP, perform the following on the base routing instance of each NE that is to participate in a VPRN:

- **a** As required, enable VPN IPv4 and VPN IPv6.
- **b** As required, enable multicast IPv4 to apply the multicast extension. See Procedure 23-2 and chapter 71 for more information.

4 Create at least one BGP peer group. See Procedure 23-4 for more information.

5 As required, create BGP neighbors with which to peer. See Procedure 23-5 for more information.

6 As required, enable or disable BGP peering. See Procedure 23-6 for more information.

23.4 Workflow to configure RIP

1 Enable RIP on the routing instance. See Procedure 23-8 for more information.

2 Configure global-level RIP. See Procedure 23-9 for more information.

3 Configure group-level RIP. See Procedure 23-10 for more information.

4 Configure neighbor-level (also known as interface) RIP. See Procedure 23-11 for more information.

23.5 Workflow to configure LDP

1 Enable LDP on the routing instance. See Procedure 23-12 for more information.

2 Configure global-level LDP. See Procedure 23-13 for more information.

3 Configure one of the following options.

a If two LDP peers are adjacent devices, create an LDP interface. See Procedure 23-14 for more information.

b If two LDP peers are non-adjacent devices, create an LDP targeted peer. See Procedure 23-16 for more information.

4 Create an LDP keychain. See Procedure 23-15 for more information.

5 As required, configure ECMP on an LDP routing interface. See Procedure 23-17 for more information.

23.6 Workflow to configure IS-IS

1 Enable IS-IS on the routing instance. See Procedure 23-19 for more information.

2 Configure global-level IS-IS. See Procedure 23-20 for more information.

3 Configure at least one NET address. See Procedure 23-22 for more information.

4 Configure at least one IS-IS interface. See Procedure 23-23 for more information.

5 As required, if LDP over RSVP is enabled for IS-IS, configure an operational LSP between routers. See chapter 25 for more information.

23.7 Workflow to configure OSPFv2 and OSPFv3

1. Enable OSPF on the routing instance. See Procedure 23-24 for more information.
2. Create at least one OSPFv2 or OSPFv3 area. See Procedure 23-25 for more information.
3. As required, create an OSPF neighbor on an OmniSwitch. See Procedure 23-26 for more information.
4. Assign Layer 3 interfaces to the routers in the OSPFv2 or OSPFv3 area. See Procedure 23-27 for more information.
5. As required, create an OSPF area range. See Procedure 23-28 for more information.
6. As required, create a virtual link between the backbone OSPF area and a remote OSPF area that does not advertise the OSPF topology. See Procedure 23-29 for more information.
7. Configure OSPF on the routing instance. See Procedure 23-30 for more information.
8. Assign routers to the OSPFv2 or OSPFv3 area. See Procedure 23-31 for more information.

23.8 Workflow to configure RSVP

1. As required, configure MPLS, LSP, MPLS path, and LSP path parameters. See chapter 25 for more information.
2. Configure the RSVP on the routing interface. See Procedure 23-32 for more information.
3. Configure the RSVP interface. See Procedure 23-33 for more information.
4. As required, enable LDP. See Procedure 23-12 for more information.

23.9 Workflow to configure L2TP

1. Configure L2TP on a routing instance. See Procedure 23-34 for more information.
2. Create and configure an LNS group and group member for an LNS site. If the site is an LAC, this configuration is not required. See Procedure 14-6 for more information.
3. As required, configure the ESM profiles for LNS L2TP termination:
   a. VPRN; see Procedure 71-60 for more information
   b. IES; see Procedure 70-12 for more information

4 As required, configure L2TP on each local user database PPPoE host to be forwarded to the LNS (applicable for the LAC and the LNS, where RADIUS is not used). See Procedure 65-5 for more information.

5 As required, view L2TP tunnels and endpoints. See Procedure 23-35 for more information.

6 As required, view L2TP tunnel instance endpoints associated with a subscriber host. See Procedure 23-36 for more information.

7 As required, view L2TP sessions. See Procedure 23-37 for more information.

8 As required, view PPP sessions on an LAC or LNS. See Procedure 23-38 for more information.

23.10 Workflow to configure PIM

1 Enable PIM on a routing instance. See Procedure 23-39 for more information.

2 Configure PIM on a routing instance. See Procedure 23-40 for more information. To configure PIM on a VPRN routing instance, see Procedure 23-41.

3 As required, configure Anycast RP for PIM on a router. See Procedure 23-42 for more information.

4 Configure a PIM interface. See Procedure 23-43 for more information.

23.11 Workflow to configure IGMP

1 Enable IGMP on the routing interface. See Procedure 23-45 for more information.

2 Configure IGMP on the routing instance.See Procedure 23-46 for more information.

3 As required, configure IGMP on an OmniSwitch. See Procedure 23-47 for more information.

4 Configure an IGMP interface. See Procedure 23-48 for more information.

5 As required, turn up or shut down an IGMP interface. See Procedure 23-49 for more information.

6 As required, view IGMP statistics, as follows:

a IGMP multicast reporting statistics; see Procedure 23-50 for more information

b IGMP source statistics; see Procedure 23-51 for more information

23.12 Workflow to configure MSDP

1. Enable MSDP on the routing instance. See Procedure 23-52 for more information.
2. Configure global MSDP on the routing instance. See Procedure 23-53 for more information.
3. Create at least one MSDP peer or group-peer.
   a. As required, configure group-level MSDP. See Procedure 23-54 for more information.
   b. As required, configure peer-level MSDP. See Procedure 23-56 for more information.
4. As required, configure group-peer-level MSDP. See Procedure 23-57 for more information.
5. As required, configure an MSDP source. See Procedure 23-55 for more information.
6. As required, enable or disable MSDP peering. See Procedure 23-58 for more information.

23.13 Workflow to configure MLD

1. Enable MLD on the routing instance. See Procedure 23-59 for more information.
2. Configure MLD on the routing instance or VPRN routing instance. See Procedure 23-60 for more information.
3. Create an MLD interface on the routing instance or VPRN routing instance. See Procedure 23-61 for more information.
4. Create an MLD interface on an IES L3 access interface. See Procedure 23-62.

23.14 Workflow to configure bridging on an OmniSwitch device

1. As required, configure bridging on an OmniSwitch. See Procedure 23-63 for more information.
2. Release a violated OmniSwitch LSP port if required. See Procedure 23-64 for more information.

23.15 Workflow to configure WPP

1. As required, enable WPP on the following routing instances:
   a. Base routing instance. See Procedure 22-1 for more information.
   b. VPRN routing instance. See Procedure 71-6 for more information.

2 Create a Web portal. See Procedure 23-65 for more information.

3 Bind a web portal to a group interface:

a IES group interface. See Procedure 70-12 for more information.

b VPRN group interface. See Procedure 71-60 for more information.

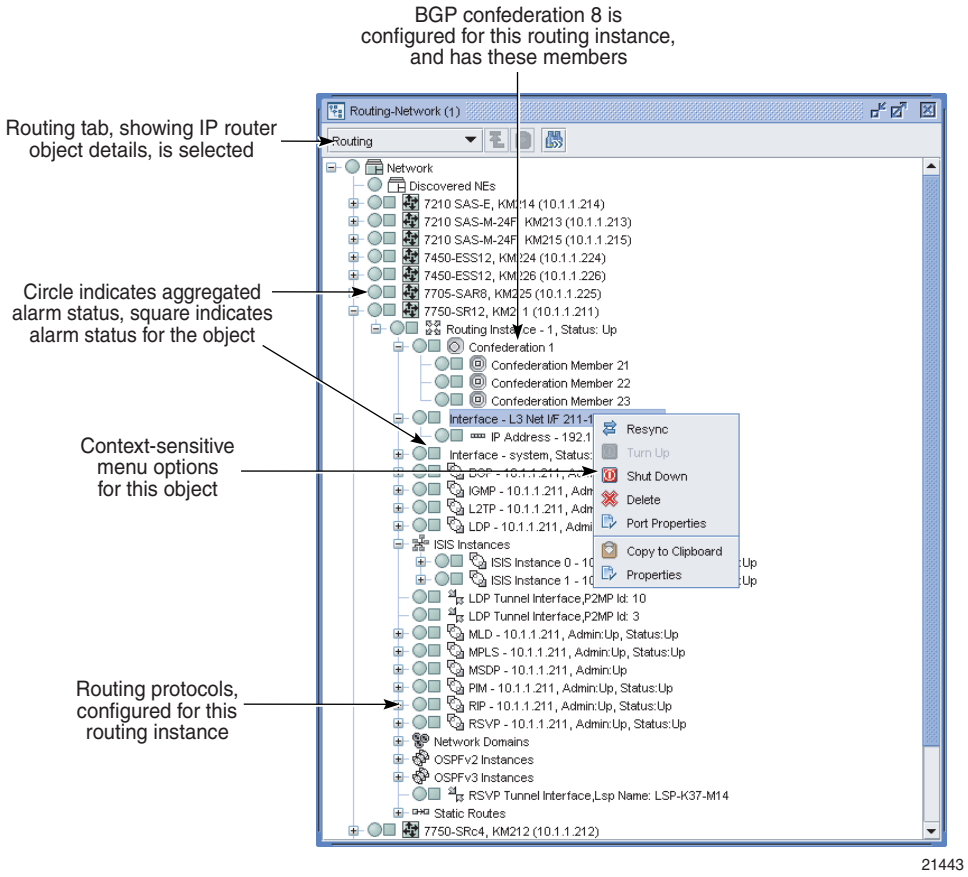
23.16 BGP configuration procedures

The BGP command hierarchy consists of three levels:

- global
- peer group
- peer (also known as neighbor)

Figure 23-6 shows the network view open to show Confederations and BGP settings.

Figure 23-6 BGP in the navigation tree network view



BGP parameters are initially applied at the global level. The parameters are inherited by the group and peer levels. Parameters can be modified and overridden on a level-specific basis.

Many of the hierarchical BGP commands can be modified at different levels. BGP group-level parameters take precedence over BGP global-level parameters. BGP peer-level parameters take precedence over group- and global-level parameters.

The following procedures describe how to configure BGP.

Procedure 23-1 To enable BGP on a routing instance

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the routing instance icon. The path is Routing→Router→Routing Instance.

3 Right-click on the routing instance icon and choose Properties. The Routing Instance (Edit) form opens with the General tab displayed.

4 Enable BGP.

i Click on the Protocols tab.

ii Choose the BGP Enabled parameter.



Note 1 — You must configure an AS number before enabling BGP. Configure the Autonomous System parameter on the Routing tab of the Routing Instance (Edit) form.

Note 2 — If a confederation is required, configure the Confederation Autonomous System parameter on the Routing tab on the Routing Instance (Edit) form.

5 Click on the OK button. The Routing Instance (Edit) form closes, a BGP entry appears in the list of enabled protocols, and a BGP icon appears in the network view of the navigation tree.

Procedure 23-2 To configure global-level BGP

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the BGP icon. The path is Routing→Router→Routing Instance→BGP.

3 Right-click on the BGP icon and choose Properties. The BGP Site (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- Description
- Router ID
- Administrative State
- Cluster ID
- Keep MP-BGP Routes

5 Assign a TCP key chain, if required.



Note — You can assign a TCP key chain to a BGP site, group, or peer on a 7950 XRS, 7750 SR, or on a 7450 ESS in mixed mode.

i Click on the Select button in the KeyChain panel. The Select BGP Site Keychain - BGP form opens.

ii Choose a key chain in the list and click on the OK button. The Select BGP Site Keychain - BGP form closes. The 5620 SAM assigns the key chain to the BGP instance.

6 Configure the parameters in the Graceful Restart panel:

- Graceful Restart
- Stale Routes Time (seconds)
- Restart Time (seconds)
- Enable Notification

The graceful restart parameters are configurable when you enable the Graceful Restart parameter.

7 Configure the parameters in the MED panel:

- MED Source
- MED Value

The parameters are used to find a way to leave the AS when there are multiple methods of leaving the AS.

8 Configure the parameters in the IGP Shortcut panel:

- IGP Shortcut
- Disallow IGP

The Disallow IGP parameter is only displayed if you enable one of the IGP Shortcut parameter options.

9 Configure the parameters in the MultiPath panel:

- Multi Path
- IBGP MultiPath
- EIBGP LoadBalance

Set the Multi Path parameter to 1 to disable. When the parameter is set from 2 to 16, multipath is enabled and BGP load shares traffic across the number of links specified. If the equal cost routes available are greater than the configured value, routes with the lowest next hop IP address are chosen.

10 Configure the Backup Path parameter in the Backup Path panel.

11 Configure the parameters in the Best Path Selection panel:

- Ignore Next Hop Metric
- Ignore Router Id
- MED Compare
- Deterministic MED
- Strict

When you set the MED Compare parameter to off, the Strict parameter is set to true and is not configurable. When you set the MED Compare parameter to on, the Strict parameter is set to false and is not configurable.

12 Configure the parameters in the OLC panel.

- Current OLC State
- Revert OLC State

13 Click on the Behavior tab.

14 Configure the parameters:

- Preference
- Local Preference
- Multi Hop
- Loop Detect
- Aggregator ID Zero
- Damping
- Disable Client Reflect
- Min. Route Advertisement
- Disable Standard Communities
- Disable Extended Communities
- Disable Fast External Failover
- Advertise Inactive Routes
- Enable Inter AS VPRN
- Enable Rapid Withdrawal
- Enable Peer Tracking
- BFD Enabled
- FlowSpec Validate Enabled
- Connect Retry Time (seconds)
- Keep Alive (seconds)
- Purge Time (minutes)
- Transport Tunnel
- Path MTU Discovery Enabled
- Disable Route Table Install
- Enable Route Reflector VPN Forwarding
- Peer Tracking Policy
- Split Horizon
- IANA MVPN VRF Import Subtype

The Enable Inter AS VPRN parameter is not configurable on a VPRN routing instance.

15 Configure the parameters in the Next-Hop Resolution panel:

- Use BGP Routes
- Policy

16 Configure the parameters in the Hold Time panel:

- Hold Time (seconds)
- Minimum Hold Time (seconds)

17 Configure the parameters in the Add-Path panel:

- Enable Add-Path Send
- Add-Path Receive
- IPv4 Add-Path Limit
- VPN IPv4 Add-Path Limit
- IPv6 Add-Path Limit
- VPN IPv6 Add-Path Limit

18 Configure the Fault Tolerance parameter in the Error Handling panel. The Fault Tolerance parameter allows BGP routers to be more tolerant of some UPDATE message errors, use less disruptive error recovery mechanisms, and provide better operational and diagnostics information.

19 Configure the parameters in the Damp Peer Oscillations panel:

- Enable Damp Peer Oscillation
- Initial Wait Time (minutes)
- Second Wait Time (minutes)
- Maximum Wait Time (minutes)
- Error Interval (minutes)

20 Click on the AS Properties tab.

21 Configure the parameters:

- Min AS Origination (seconds)
- Disable 4Byte ASN

22 Configure the parameters in the Local AS panel:

- Local AS
- Private
- No Prepend Global AS

The No Prepend Global AS is configurable only if you set the Local AS parameter to a value other than 0.

The Local AS parameters are used to configure a virtual AS. A virtual AS is used when a router (RTA) is moved from one AS (AS1) to another AS (AS2). However, the customer router (CR1) is configured to belong to the AS1. To avoid reconfiguring CR1 to belong to AS2, CR1 can continue to belong to AS1, but RTA has its local AS value set to AS1. RTA can advertise AS1 for routes advertised to CR1.

23 Configure the parameters in the Remove Private AS panel:

- Remove Private AS
- Limited

24 Click on the VPN tab.

25 Configure the parameters in the VPN panel:

- Family
- Apply Import Route Policies
- Apply Export Route Policies
- AS Override

If you are configuring global-level BGP for BGP AD in VPLS or for BGP VPLS, you must enable the L2 VPN option for the Family parameter.

The Apply Import Route Policies and Apply Export Route Policies parameters are not configurable on a VPRN routing instance.

The Apply Import Route Policies and Apply Export Route Policies parameters specify whether to apply the existing import and export route policies configured on the Import Policies and Export Policies tabs.

26 Configure the parameters in the AS Path Ignore panel:

- AS Path Ignore
- AS Path Ignore Family

The AS Path Ignore Family parameter is configurable when the AS Path Ignore parameter is set to true.

27 Configure the Address Family parameter in the Rapid Update panel.

28 Configure the Address Family parameter in the Advertise External panel.

29 Add a peer group, if required.

i Click on the Group tab.

ii Click on the Create button.The Peer Group (Create) form opens.

iii Perform steps 4 to 29 of Procedure 23-4.

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Peer Group (Create) form closes.

30 Add a peer, if required.

i Click on the Peer tab.

ii Click on the Create button. The Peer (Create) form opens.

iii Perform steps 4 to 30 of Procedure 23-5.

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Peer (Create) form closes.

31 Click on the Import Policies tab.

32 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5
- Policy 6
- Policy 7
- Policy 8
- Policy 9
- Policy 10
- Policy 11
- Policy 12
- Policy 13
- Policy 14
- Policy 15

Configure the import route policies to determine which routes are accepted from peers. The policies should match the policies you configure using the Routing Policy Manager, as described in chapter 22. There is no validation performed by the router to ensure the policies match.

33 Click on the Export Policies tab.

34 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5
- Policy 6
- Policy 7
- Policy 8
- Policy 9
- Policy 10
- Policy 11
- Policy 12
- Policy 13
- Policy 14
- Policy 15

Configure the export route policies to determine which routes are advertised to peers. The policies should match the policies you configure using the Routing Policy Manager, as described in chapter 22. A router performs no validation to ensure the policies match.

35 Click on the Authentication tab.

36 Configure the parameters:

- Type
- Key

37 Click on the following tabs to view information:

- Statistics
- Faults

38 Click on the OK button. The BGP (Edit) form closes.

Procedure 23-3 To configure a BGP confederation

For BGP confederations, the following rules apply:

- A device can only belong to one confederation.
- Multiple devices can belong to one BGP confederation.

You must configure BGP on the device and configure global-level BGP parameters before you configure BGP confederations, as described in Procedures 23-1 and 23-2.

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the routing instance icon. The path is Routing→Router→Routing Instance.

3 Right-click on the Routing Instance icon and choose Properties. The Routing Instance (Edit) form opens.

4 Click on the Routing tab.

5 Enter the confederation number for the Confederation Autonomous System parameter and click on the Apply button.

6 Click on the BGP Confederations tab.

7 Click on the Create button to add a BGP confederation, or choose a BGP confederation from the list and click on the Properties button to configure an existing BGP confederation. The Confederation (Edit) form opens with the General tab displayed.



Note — You can only have one BGP confederation per device.

8 To add a new member to the confederation:

i Click on the Members tab.

ii Click on the Create button. The Confederation Member (Create) form opens.

iii Configure the Member AS parameter as the number of ASs for the confederation. The member AS number represents the BGP instance of the device.

iv Click on the OK button. The Confederation Member (Create) form closes, and an entry for the new confederation member AS appears in the Confederation (Edit) form.

9 Click on the OK button. The Confederation (Edit) form closes and the Routing Instance (Edit) reappears. A Confederation icon appears in the Navigation Tree below the Routing Instance icon.

You can verify the confederation membership by opening the Confederation icon to view icons that represent the members of the confederation as specified in step 8.

10 Close the Routing Instance (Edit) form.

Procedure 23-4 To configure peer-group-level BGP



Note 1 — For most parameters in this procedure, you can specify that the parameter value is inherited from the parent BGP configuration using the Inherit Value parameter.

If you disable value inheritance for a parameter, the available options are restricted, based on the parent parameter value and the protocol functionality. For example, if a parameter in the global-level BGP configuration is set to True, the only available option for the same parameter in the peer-group-level BGP configuration is False, unless a value of False violates a protocol rule, in which case the only available option is True.

Note 2 — The parameters that you configure for a BGP peer group take precedence over the parameters that are configured for global-level BGP.

1 Choose Routing from the navigation tree view selector from the 5620 SAM GUI.

2 Choose Routing→Router→Routing Instance→BGP.

3 Right-click on the BGP icon and choose Create Group. The Peer Group (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Name
- Description
- Administrative State
- Cluster ID
- Local Address
- Inherit Value
- Dynamic Peer

5 Assign a TCP key chain, if required.



Note — You can assign a TCP key chain to a BGP site, group, or peer on a 7950 XRS, 7750 SR, or on a 7450 ESS in mixed mode.

i Click on the Select button in the KeyChain panel. The Select BGP Group Keychain - Peer Group form opens.

ii Choose a key chain in the list and click on the OK button. The Select BGP Group Keychain - Peer Group form closes. The 5620 SAM assigns the key chain to the BGP peer group.

6 Configure the parameters in the Graceful Restart panel:

- Graceful Restart
- Stale Routes Time (seconds)
- Restart Time (seconds)
- Enable Notification
- Inherit Value

The graceful restart parameters are configurable when the Graceful Restart parameter is enabled.

The Graceful Restart parameter is not configurable on 7210 SAS-M and 7210 SAS-X devices.

7 Configure the parameters in the MED panel:

- MED Source
- MED Value
- Inherit Value

The parameters are used to find a way to leave the AS when there are multiple methods of leaving the AS.

8 Click on the Apply button.

9 Configure the parameters in the OLC panel:

- Current OLC State
- Revert OLC State

10 Click on the Behavior tab.

11 Configure the parameters:

- Preference
- Local Preference
- Multi Hop
- Loop Detect
- Aggregator ID Zero
- Damping
- Disable Client Reflect
- Min. Route Advertisement
- Disable Standard Communities
- Disable Extended Communities
- Disable Fast External Failover
- Advertise Inactive Routes
- Enable Peer Tracking
- BFD Enabled
- FlowSpec Validate Enabled
- Connect Retry Time (seconds)
- Keep Alive (seconds)
- Peer Type
- Passive
- Next Hop Self
- Minimum TTL Value
- Path MTU Discovery Enabled
- Default Route Target
- Accumulated IGP
- Split Horizon
- Next Hop Unchanged

12 Configure the parameters in the Hold Time panel:

- Hold Time (seconds)
- Minimum Hold Time (seconds)

13 Configure the parameters in the Prefix Limit panel:

- Prefix Limit
- Log Only
- Threshold
- Idle Timeout
- Never Timeout

The Idle Timeout parameter is configurable when the Never Timeout parameter is disabled.

14 Configure the parameters in the Add Path panel:

- Enable Add-Path Send
- Add-Path Receive
- IPv4 Add-Path Limit
- VPN IPv4 Add-Path Limit
- IPv6 Add-Path Limit
- VPN IPv6 Add-Path Limit
- Inherit Value

15 Configure the parameters in the Error Handling panel. The Fault Tolerance parameter allows BGP routers to be more tolerant of certain UPDATE message errors, use less disruptive error recovery mechanisms, and provide better operational and diagnostics information.

- Fault Tolerance
- Inherit Value

16 Configure the parameters in the Damp Peer Oscillations panel:

- Enable Damp Peer Oscillation
- Initial Wait Time (minutes)
- Second Wait Time (minutes)
- Maximum Wait Time (minutes)
- Error Interval (minutes)
- Inherit Value

17 Click on the AS Properties tab.

18 Configure the parameters:

- Peer AS
- Min AS Origination (seconds)
- Disable 4Byte ASN
- AS Override
- Inherit Value

The Peer AS parameter specifies the peer AS for this specific group, and the behavior, internal or external. Multipath configurations are not supported at the BGP peer level.

19 Configure the parameters in the Local AS panel:

- Local AS
- Private
- No Prepend Global AS
- Inherit Value

The No Prepend Global AS is configurable only if you set the Local AS parameter to a value other than 0.

The Local AS parameters are used to configure a virtual AS. A virtual AS is used when a router (RTA) is moved from one AS (AS1) to another AS (AS2). However, the customer router (CR1) is configured to belong to the AS1. To avoid reconfiguring CR1 to belong to AS2, CR1 can continue to belong to AS1, but RTA has its local AS value set to AS1. RTA can advertise AS1 for routes advertised to CR1.

20 Configure the parameters in the Remove Private AS panel:

- Remove Private AS
- Limited
- Inherit Value

21 Click on the VPN tab.

22 Configure the parameters in the VPN panel:

- Family
- Apply Import Route Policies
- Apply Export Route Policies
- Inherit Value



Note 1 — The Advertise Label, Apply Import Route Policies, and Apply Export Route Policies parameters are not configurable for a VPRN routing instance.

Note 2 — The Apply Import Route Policies and Apply Export Route Policies parameters specify whether to apply the existing import and export route policies configured on the Import Policies and Export Policies tabs.

23 Add a peer, if required.

i Click on the Peer tab.

ii Click on the Create button. The Peer (Create) form opens.

iii Perform steps 4 to 30 of Procedure 23-5.

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Peer (Create) form closes.

24 Click on the Import Policies tab.

25 Configure the parameters:

- Inherit Value
- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5
- Policy 6
- Policy 7
- Policy 8
- Policy 9
- Policy 10
- Policy 11
- Policy 12
- Policy 13
- Policy 14
- Policy 15

Configure the import route policies to determine which routes are accepted from peers. The policies should match the policies you configure using the Routing Policy Manager, as described in chapter 22. There is no validation performed by the router to ensure the policies match.

26 Click on the Export Policies tab.

27 Configure the parameters:

- Inherit Value
- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5
- Policy 6
- Policy 7
- Policy 8
- Policy 9
- Policy 10
- Policy 11
- Policy 12
- Policy 13
- Policy 14
- Policy 15



Note — Configure the export route policies to determine which routes are advertised to peers. The policies should match the policies you configure using the Routing Policy Manager, as described in chapter 22. A router performs no validation to ensure the policies match.

28 Click on the Authentication tab.

29 Configure the parameters:

- Type
- Key
- Inherit Value

30 Click on the following tabs to view information.

- Statistics
- Faults

31 Click on the OK button. The Peer Group (Create) form closes, and the 5620 SAM displays an icon for the new peer group under the BGP icon in the navigation tree.

Procedure 23-5 To configure peer-level BGP



Note 1 — For most parameters in this procedure, you can specify that the parameter value is inherited from the parent BGP configuration using the Inherit Value parameter.

If you disable value inheritance for a parameter, the available options are restricted, based on the parent parameter value and the protocol functionality. For example, if a parameter in the peer-group-level BGP configuration is set to True, the only available option for the same parameter in the peer-level BGP configuration is False, unless a value of False violates a protocol rule, in which case the only available option is True.

Note 2 — The parameters that you configure for a BGP peer take precedence over the parameters that are configured for group-level BGP.

1 Choose Routing from the navigation tree view selector from the 5620 SAM GUI.

2 Choose Routing→Router→Routing Instance→BGP→Peer Group.

3 Right-click on the peer group icon and choose Create Peer. The Peer (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Description
- Peer Address
- Administrative State
- Cluster ID
- Local Address
- Inherit Value

5 Configure the parameters in the Graceful Restart panel:

- Graceful Restart
- Stale Routes Time (seconds)
- Restart Time (seconds)
- Enable Notification
- Inherit Value

The graceful restart parameters are configurable when the Graceful Restart parameter is enabled.

6 Configure the parameters in the MED panel:

- MED Source
- MED Value
- Inherit Value

The parameters are used to find a way to leave the AS when there are multiple methods of leaving the AS.

7 Click on the Apply button.

8 Configure the parameters in the OLC panel.

- Current OLC State
- Revert OLC State

9 Click on the Behavior tab.

10 Configure the parameters:

- Preference
- Local Preference
- Multi Hop
- Loop Detect
- Aggregator ID Zero
- Damping
- Disable Client Reflect
- Min. Route Advertisement
- Disable Standard Communities
- Disable Extended Communities
- Disable Fast External Failover
- Advertise Inactive Routes
- Enable Peer Tracking
- BFD Enabled
- Connect Retry Time (seconds)
- Keep Alive (seconds)
- Peer Type
- Passive
- Next Hop Self
- Minimum TTL Value
- Path MTU Discovery Enabled
- Default Route Target
- Accumulated IGP
- Inherit Value
- FlowSpec Validate Enabled
- Split Horizon

11 Configure the parameters in the Hold Time panel:

- Hold Time (seconds)
- Minimum Hold Time (seconds)
- Inherit Value

12 Configure the parameters in the Prefix Limit panel:

- Prefix Limit
- Log Only
- Threshold
- Idle Timeout
- Inherit Value

13 Configure the parameters in the Add-Path panel:

- Enable Add-Path Send
- Add-Path Receive
- IPv4 Add-Path Limit
- VPN IPv4 Add-Path Limit
- IPv6 Add-Path Limit
- VPN IPv6 Add-Path Limit
- Inherit Value

14 Configure the parameters in the Error Handling panel. The Fault Tolerance parameter allows BGP routers to be more tolerant of certain UPDATE message errors, use less disruptive error recovery mechanisms, and provide better operational and diagnostics information.

- Fault Tolerance
- Inherit Value

15 Configure the parameters in the Damp Peer Oscillations panel:

- Enable Damp Peer Oscillation
- Initial Wait Time (minutes)
- Second Wait Time (minutes)
- Maximum Wait Time (minutes)
- Error Interval (minutes)
- Inherit Value

16 Click on the AS Properties tab.

17 Configure the parameters:

- Peer AS
- Min AS Origination (seconds)
- Disable 4Byte ASN
- Inherit Value

The Peer AS parameter specifies the peer AS for the group to which the peer belongs, and the behavior, internal or external. Multipath configurations are not supported at the BGP peer level.

18 Configure the parameters in the Local AS panel:

- Local AS
- Private
- No Prepend Global AS
- Inherit Value

The No Prepend Global AS parameter is configurable when you set the Local AS parameter to a value other than 0.

19 Configure the parameters in the Remove Private AS panel:

- Remove Private AS
- Limited
- Inherit Value

20 Click on the VPN tab.

21 Configure the parameters:

- Family
- Advertise Label
- Advertise LDP Prefix
- Apply Import Route Policies
- Apply Export Route Policies
- Inherit Value

The Advertise LDP Prefix is only displayed when the Advertise Label parameter is enabled for IPv4 routes.

The Apply Import Route Policies and Apply Export Route Policies parameters specify whether to apply the existing import and export route policies configured on the Import Policies and Export Policies tabs.

22 Click on the Graceful Restart tab.

23 Configure the parameters:

- Graceful Restart
- Stale Routes Time (seconds)
- Inherit Value

24 Assign a TCP key chain, if required.



Note — You can assign a TCP key chain to a BGP site, group, or peer on a 7950 XRS, 7750 SR, or on a 7450 ESS in mixed mode.

i Click on the KeyChain tab.

ii Click on the Select button. The Select BGP Peer Keychain - Peer form opens.

iii Choose a key chain in the list and click on the OK button. The Select BGP Peer Keychain - Peer form closes and the 5620 SAM assigns the key chain to the BGP peer.

25 Click on the Import Policies tab.

26 Configure the parameters:

- Inherit Value
- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5
- Policy 6
- Policy 7
- Policy 8
- Policy 9
- Policy 10
- Policy 11
- Policy 12
- Policy 13
- Policy 14
- Policy 15

Configure the import route policies to determine which routes are accepted from peers. The policies should match the policies you configure using the Routing Policy Manager, as described in chapter 22. There is no validation performed by the router to ensure the policies match.

27 Click on the Export Policies tab.

28 Configure the parameters:

- Inherit Value
- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5
- Policy 6
- Policy 7
- Policy 8
- Policy 9
- Policy 10
- Policy 11
- Policy 12
- Policy 13
- Policy 14
- Policy 15

Configure the export route policies to determine which routes are advertised to peers. The policies should match the policies you configure using the Routing Policy Manager, as described in chapter 22. A router performs no validation to ensure the policies match.

29 Click on the Authentication tab.

30 Configure the parameters:

- Type
- Key
- Inherit Value

31 Click on the OK button. The Peer (Create) form closes and a Peer icon appears below the Peer Group icon in the Navigation Tree of the network view.

32 Configure the protocol for the far-end device, if applicable. Use CLI for devices that are managed outside the scope of the 5620 SAM.

Procedure 23-6 To enable or disable BGP peering

1 Choose Routing from the navigation tree view selector from the 5620 SAM GUI.

2 Choose Routing→Router→Routing Instance→BGP→Peer Group.

3 Click on the Peer Group icon to display the peers in the peer group.

4 Right-click on a peer and choose one of the following menu items:

a Turn Up to activate a peer

b Shut Down to deactivate a peer

5 A dialog box appears. Click on the Yes button. The state information beside the Peer icon changes accordingly.

Procedure 23-7 To perform a routing policy test

Perform the following procedure to verify BGP routes against a routing policy. The output of the test returns the prefixes that are accepted and rejected by the policy. This test allows you to evaluate an existing routing policy against the RIB to identify the prefixes that are matched or not matched by the policy, before attaching the prefix to a routing neighbor or instance.

1 Perform one of the following:

   a Perform a routing policy test on a base router instance BGP site.

      i From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

      ii Navigate to the BGP icon. The path is Routing→NE→Routing Instance→BGP.

      iii Right-click on the BGP and choose Routing Policy Test. The rtr BGP Routing Policy Test form opens.

   b Perform a routing policy test on a VPRN instance BGP site.

      i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

      ii Configure the filter criteria. A list of services appears.

      iii Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens.

      iv Navigate to the BGP Site icon in the service navigation tree. The path is Sites→Routing Instance - NE System ID→Routing Instance→Protocol s→BGP Site.

      v Right-click on the BGP Site icon and choose Routing Policy Test. The VPRN BGP Routing Policy Test form opens.

2 Configure the parameters:

- Policy Name
- Family
- RD
- Prefix
- Longer Prefix Match
- Neighbor
- Display Rejects
- Output Format

   You must enter the name of an existing and distributed routing policy for the Policy Name parameter.

3 Click on the Execute button and view the results.

4 Click on the Close button.

23.17 RIP configuration procedures

The RIP command hierarchy consists of three levels:

- global
- group
- interface (also known as neighbor)

For RIP configuration, you must define at least one group and one interface. The parameters that are configured on the global level are inherited by the group and interface levels. Parameters can be modified and overridden on a level-specific basis.

Many of the hierarchical RIP commands can be modified on different levels. RIP group-level parameters take precedence over BGP global-level parameters. RIP interface-level parameters take precedence over peer-group and global-level parameters.

When configuring RIP on the 7705 SAR, a RIP routing site is created under the routing instance which can be seen in the routing network tree. Using this RIP routing site, RIP groups and RIP interfaces can be configured.

The following procedures describe how to configure RIP.

Procedure 23-8 To enable RIP on a routing instance

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the routing instance icon. The path is Routing→Router→Routing Instance.

3 Right-click on the routing instance icon and choose Properties. The Routing Instance (Edit) form opens.

4 Enable RIP.

  i Click on the Protocols tab.

  ii Select the RIP Enabled parameter.

5 Click on the OK button to save the changes. A dialog box appears.

6 Click on the Yes button. The Routing Instance (Edit) form closes, and a RIP icon appears under the routing instance in the navigation tree.

Procedure 23-9 To configure global-level RIP

1 Choose Routing from the navigation tree view selector from the 5620 SAM GUI.

2 Choose Routing→Router→Routing Instance→RIP.

3 Right-click on the RIP icon and choose Properties. The RIP Site (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- Description
- Administrative State

5 Click on the Behavior tab.

6 Configure the parameters:

- Check Zero
- Message Size
- Metric In
- Metric Out
- Preference
- Receive
- Send
- Split Horizon
- Propagate RIP Metric
- Flush
- Timeout
- Update

The Send parameter specifies the type of messages received based on the RIP version, and the variation of RIPv2 messages sent, broadcast or multicast.

The Propagate RIP Metric parameter is configurable only when configuring RIP on a VPRN routing instance.

7 Click on the Authentication tab.

8 Configure the parameters:

- Type
- Key

9 Click on the Import Policies tab.

10 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Specify routing policies that determine the routes that RIP interfaces import. You can specify up to five routing policies. The routing policies are enforced in order, from one to five.

11 Click on the Export Policies tab.

12 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Specify routing policies that determine the routes that RIP interfaces export. You can specify up to five routing policies. The routing policies are enforced in order, from one to five.

13 To create a RIP group, click on the Group tab.

i Click on the Create button. The RIP Group (Create) form opens.

ii Configure the parameters. See Procedure 23-10 for more information.

14 Click on the Interface tab. To configure interface-level (also known as neighbor) RIP parameters:

i Click on the Create button. The RIP Interface (Create) form opens.

ii Configure the parameters. See Procedure 23-11 for more information.

15 Click on the following tabs to view statistics and alarm information.

- Statistics
- Faults

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The RIP Site (Edit) form closes.

Procedure 23-10 To configure group-level RIP



Note 1 — You can choose to inherit values from the global-level RIP configuration by selecting the Inherit Value parameter. If you choose not to inherit a parameter value from the global-level RIP configuration, only the parameter options that are not set in the parent configuration are available. For example, if the Check Zero parameter is set to false in the global-level RIP configuration, you can only set the parameter to true in the group-level RIP configuration.

Note 2 — The parameters that you configure for a RIP group take precedence over the parameters that are configured for the global-level RIP configuration.

1 Choose Routing from the navigation tree view selector.

2 Navigate to the RIP icon. The path is Routing→Router→Routing Instance→RIP.

3 Right-click on the RIP icon and choose Create Group. The RIP Site Group (Create) form opens with the General tab displayed.

4 Configure the Name parameter.

5 Perform steps 4 to 12 of Procedure 23-9.

6 Click on the OK button. The RIP Group (Create) form closes, and the 5620 SAM displays an icon for the new RIP group in the navigation tree below the RIP icon.

Procedure 23-11 To configure interface-level RIP



Note 1 — You can choose to inherit values from the global-level RIP configuration by selecting the Inherit Value parameter. If you choose not to inherit a parameter value from the global-level RIP configuration, only the parameter options that are not set in the parent configuration are available. For example, if the Check Zero parameter is set to false in the global-level RIP configuration, you can only set the parameter to true in the interface-level RIP configuration.

Note 2 — The parameters that you configure for a RIP interface, also known as a RIP neighbor, take precedence over the parameters that are configured for the group- and global-level RIP configuration.

1 Choose Routing from the navigation tree view selector.

2 Navigate to a RIP group. The path is Routing→Router→Routing Instance→RIP→RIP Group.

3 Right-click on the RIP group icon and choose Create Interface. The RIP Interface (Create) form opens with the General tab displayed.

4 Perform steps 4 to 12 of Procedure 23-9.

5 Click on the OK button. The RIP Interface (Create) form closes, and the 5620 SAM displays an icon for the new RIP interface below the RIP group icon in the navigation tree.

23.18 LDP configuration procedures

An LDP instance in the 5620 SAM network navigation tree has the following child objects:

- Interfaces–The interfaces object contains the configured LDP interfaces for directly connected peers. The 7210 SAS-M does not support configuration of LDP interfaces.
- Targeted Peers–The targeted peers object contains the indirectly connected peers.

T-LDP is supported on the 7950 XRS, 7750 SR, 7710 SR, 7450 ESS, 7210 SAS-M, 7210 SAS-X, and 7705 SAR. DU-LDP is supported on the 7750 SR and 7705 SAR.

The following procedures describe how to configure LDP.

Procedure 23-12 To enable LDP on a routing instance

1 Choose Routing from the navigation tree view selector.

2 Navigate to the routing instance icon. The path is Routing→Router→Routing Instance.

3 Right-click on the routing instance icon and choose Properties. The Routing Instance (Edit) form opens.

4 Enable LDP.

i Click on the Protocols tab.

ii Select the LDP Enabled parameter.

5 Click on the OK button to save the changes. A dialog box appears.

6 Click on the Yes button. The Routing Instance (Edit) form closes, and an LDP icon appears under the routing instance in the navigation tree.

Procedure 23-13 To configure global-level LDP

1 Enable LDP on the router, as described in Procedure 23-12.

2 Choose Routing from the navigation tree view selector.

3 Navigate to the LDP instance icon. The path is Routing→Router→Routing Instance→LDP.

4 Right-click on the LDP icon and choose Properties. The LDP - Routing Instance (Edit) form appears, with the General tab displayed.

5 Configure the Administrative State parameter.

6 Click on the Common tab.

7 Configure the parameters:

- Targeted Sessions Allowed
- Prefer Tunnel-in-Tunnel
- Tunnel Down Damp Time (seconds)
- Enable Implicit Null Label
- Enforce Graceful Restart
- Multi Path Make Before Break Time (seconds)
- Neighbor Liveness Time (seconds)
- Maximum Recovery Time (seconds)
- Forward State Holding Time (seconds)
- Reconnect Time (seconds)
- Shortcut Local TTL Propagate
- Shortcut Transit TTL Propagate
- Fast Re-route

Configure the Targeted Sessions Allowed parameter to true to configure the router for T-LDP. Targeted sessions are LDP sessions that distribute labels between indirectly connected peers.

The Neighbor Liveness Time (seconds) and Maximum Recovery Time (seconds) parameters are configurable when the Enforce Graceful Restart parameter is enabled.

8 Click on the Interface Properties tab.

9 Configure the parameters:

- Address Type
  - Choose system to have the system IP address set up LDP sessions.
  - Choose interface to have the IP interface address set up LDP sessions only if there are not multiple interfaces between the two neighbors.
- Keep-Alive Factor
- Keep-Alive Timeout (seconds)
- Hello Factor
- Hello Timeout (seconds)

By default, these parameter values are inherited by all LDP interfaces.

10 Click on the Targeted Peer Properties tab.

i Configure the parameters:

- Keep-Alive Factor
- Keep-Alive Timeout (seconds)
- Hello Factor
- Hello Timeout (seconds)
- Enable Hello Reduction
- Hello Reduction Factor

By default, these parameter values are inherited by all LDP targeted peers.



Note — If the Enable Hello Reduction parameter is disabled while the targeted LDP session to the peer is operationally up, the change in the hold time will take effect only when the targeted LDP session is re-established.

ii Click on the Route Import Policy tab.

iii Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

iv Click on the Route Export Policy tab.

v Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

11 Click on the Ecmp OAM tab. The General tab displayed. See Procedure 23-17 for more information about configuring ECMP for LDP interfaces.

12 Click on the Interfaces tab. A list of interfaces you can view or configure opens. See Procedure 23-14 for more information about configuring LDP interfaces.

13 Click on the Peers tab. A list of peers you can view or configure opens. See Procedure 23-17 for more information about creating peers.

14 Click on the Targeted Peers tab. A list of targeted peers you can view or configure opens. See Procedure 23-16 for more information about creating and configuring targeted peers.

15 Click on the Import Policies tab.

16 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

17 Click on the Export Policies tab.

18 Configure the parameters on the General tab:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

19 Click on the Tunnel Table tab.

20 Configure the parameters on the Tunnel Table tab:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

The tunnel table policies are used to allow LDP-capable PE devices to offer services to PE routers in areas or domains where BGP-labeled routes are not supported. They are used to determine which routes are advertised to LDP. Only policy entries supporting the LDP protocol are considered; all other policies are ignored. See also Procedure 23-5 for information on enabling the advertisement of LDP prefixes to BGP peers.

21 Click on the Static Prefix FECs tab.

i Click on the Create button. The StaticFec (Create) form opens.

ii Configure the parameters:

- IP Prefix
- Probe Interval (Minutes)
- Advertised Label
- Next Hop Type
- Next Hop
- Swap Label

Next Hop Address and Swap Label parameters appear when IP Address is selected for the Next Hop Address value.

iii Click on the OK button. A dialog box appears.

iv Click on the Yes button. The static FEC form closes and the static FEC entry appears in the list.

22 Click on the Aggregate Prefix Match tab.

23 Configure the parameters:

- Aggregate Prefix Match Enabled
- Administrative State

When the Aggregate Prefix Match Enabled parameter is enabled, the LDP installs a prefix binding in the LDP FIB by performing a longest match against an aggregate prefix in the routing table, as opposed to requiring an exact match of the prefix. The LDP prefix binding continues to be advertised on a per individual /32 prefix basis.

The Administrative State parameter can only be configured if the Aggregate Prefix Match Enabled parameter is enabled.

24 Configure the following parameters in the Prefix Exclude Policies panel:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

The Prefix Exclude Policies can only be configured if the Aggregate Prefix Match Enabled parameter is enabled.

When routing policy statements are specified in the Prefix Exclude Policies panel, any prefixes defined in the routing policies are excluded from the aggregate prefix matching procedure. In this case, when LDP receives a FEC-label binding for this prefix, it performs an exact match of a specific FEC element prefix, as opposed to a longest match of one or more LDP FEC element prefixes.

25 Click on the Accounting tab.

26 Click on the Create button. The AccountingFecPrefix (Create) form opens.

27 Configure the FEC Prefix parameter.

28 Configure the parameters in the Egress Accounting Statistics panel:

- Click on the Select button. The Select Accounting Policy - AccountingFecPrefix form opens. Choose the required accounting policy and click on the OK button. Only accounting policies with the CombinedLdpLspEgressStats stats type are available for selection.
- Collect Accounting Statistics
- Administrative State

See the *5620 SAM Statistics Management Guide* for general information about configuring and collecting statistics.

29 Click on the following tabs to view LDP statistics and alarm information.

- Statistics
- Faults

30 Click on the OK button. The LDP (Edit) form closes.

Procedure 23-14 To configure an LDP interface



Note — You can choose to inherit values from the global-level LDP configuration by selecting the Inherit Value parameter.

1 Choose Routing from the navigation tree view selector.

2 Navigate to an LDP instance. The path is Routing→Router→Routing Instance→LDP.

3 Right-click on the LDP instance and choose Create Interface. The LDP Interface configuration form opens with the General tab displayed.

4 Click on the Select button to choose a Layer 3 interface. The Select Interface - LDP Interface form opens.

5 Configure the filter criteria. A list of the available interfaces appears.

6 Choose an interface in the list and click on the OK button.

7 Configure the parameters:

- Description
- Administrative State

8 Click on the Protocol Properties tab.

9 Configure the parameters:

- Keep-Alive Factor
- Keep-Alive Timeout (seconds)
- Hello Factor
- Hello Timeout (seconds)
- Address Type
- Local LSR ID
- Enable BFD Tracking
- Multicast Forwarding

By default, these parameter values are inherited by all LDP interfaces.

For the Address Type parameter:

- Choose system to have the system IP address set up LDP sessions.
- Choose interface to have the IP interface address set up LDP sessions only if there are not multiple interfaces between the two neighbors.

10 If you set the Local LSR ID parameter to Interface in step 9, perform the following to specify a routing interface:

i Click on the Select button in the Interface panel. The Select Interface form opens.

ii Configure the filter criteria, as required, and click on the Search button.

iii Select a routing interface in the list and click on the OK button. The Select Interface form closes.

11 Click on the OK button. The LPD Interface (Create) form closes, and an icon for the new LDP interface appears in the navigation tree list of interfaces below the LDP icon.

12 Click on the OK button. An icon for the new LDP interface appears in the navigation tree below the LDP icon.

13 Configure the protocol for the far-end device, if applicable. Use CLI for devices that are managed outside the scope of the 5620 SAM.

Procedure 23-15 To configure an LDP peer

1 Choose Routing from the navigation tree view selector.

2 Navigate to an LDP interface. The path is Routing→Router→Routing Instance→LDP.

3 Right-click on the LDP icon and choose Properties. The LDP (Edit) form opens.

4 Click on the Peers tab.

5 Click on the Create button. The Peer (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Peer Address
- Minimum TTL Value
- DoD Label Distribution
- Path MTU Discovery Enabled
- FEC 129 CISCO Interop
- Distribute Local Addresses Only
- PE ID MAC Flush Interop

7 Assign a TCP key chain to the LDP peer, if required.

i Click on the KeyChain tab.

ii Click on the Select button. The Select LDP Peer Keychain - Peer form opens with a list of local key chains displayed.

iii Choose a key chain in the list and click on the OK button. The Select LDP Peer Keychain - Peer form closes. The 5620 SAM assigns the key chain to the LDP peer.

8 Click on the Authentication tab.

9 Configure the parameters:

- Type
- Key

10 Click on the Import Policies tab.

The FEC prefix Import Policy provides a mean of controlling which FEC prefixes received from other LDP and T-LDP peers should be re-distributed to this LDP peer. If no policy name is specified, the NE will import all FEC prefixes it learns from other LDP and T-LDP peers to this LDP peer.

11 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

12 Click on the Export Policies tab.

The FEC prefix Export Policy provides a mean of controlling which FEC prefixes from this peer should be re-distributed to all other LDP and T-LDP peers. If no policy name is specified, the NE will export all FEC prefixes it learns from this LDP peer to all other LDP and T-LDP peers.

13 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

14 Click on the OK button. A dialog box appears.

15 Click on the Yes button. The new peer appears in the list.

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The LDP (Edit) form closes.

Procedure 23-16 To configure an LDP targeted peer



Note 1 — You can choose to inherit values from the global-level LDP configuration by selecting the Inherit Value parameter.

Note 2 — The parameters that you configure for a targeted peer take precedence over the parameters that are configured for the global-level LDP configuration.

1 Choose Routing from the navigation tree view selector.

2 Navigate to an LDP interface. The path is Routing→*NE*→Routing Instance→LDP.

3 Perform one of the following.

a Right-click on the LDP icon and choose Create Targeted Peer to create an LDP targeted peer. The Targeted Peer (Create) configuration form opens with the General tab displayed.

b Expand the LDP and Targeted Peers icons and right-click on a targeted peer. Choose Properties from the contextual menu. The Targeted Peer (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- Peer Address
- Description
- Administrative State

The Peer Address parameter is not configurable if you are modifying an existing targeted peer.

5 Click on the Protocol Properties tab.

i Configure the parameters:

- Tunneling Enabled
- BFD Enabled
- Keep-Alive Factor
- Keep-Alive Timeout (seconds)
- Hello Factor
- Hello Timeout (seconds)
- Enable Hello Reduction
- Hello Reduction Factor

By default, these parameter values are inherited from the global-level LDP instance.



Note 1 — If the Enable Hello Reduction parameter is disabled while the targeted LDP session to the peer is operationally up, the change in the hold time will take effect only when the targeted LDP session is re-established.

Note 2 — The parameters are not configurable if you are modifying an auto-created LDP targeted peer that was created using a CLI template. You can determine whether a targeted peer was automatically created on the NE using a template by verifying the Creator indicator.

ii Click on the Select button to configure the Local LSR ID. The Select Local LSR ID form opens.

iii Choose a Local LSR ID from the list and click the OK button. The Select Local LSR ID form closes and the name of the Local LSR ID you chose appears in the Name field.

6 If you are creating an LDP targeted peer, click on the LSPs tab. Otherwise, go to step 7. View, add, or configure associated LSPs, as required.

See chapter 25 for information on creating and configuring LSPs.

7 Click on the OK button. The Targeted Peer (Create|Edit) form closes, and an icon for the new LDP targeted peer appears in the navigation tree list of targeted peers below the LDP icon.

8 Configure the protocol for the far-end device, if applicable. Use CLI for devices that are managed outside the scope of the 5620 SAM.

Procedure 23-17 To configure ECMP for LDP routing



Note — 5620 SAM supports LDP ECMP when LDP routing is configured on the 7950 XRS, 7750 SR, 7450 ESS, 7710 SR and 7705 SAR.

1 Choose Routing from the navigation tree view selector.

2 Navigate to an LDP interface. The path is Routing→Router→Routing Instance→LDP.

3 Right-click on the LDP icon and choose Properties. The LDP Routing Instance (Edit) form opens.

4 Click on the ECMP OAM tab.

5 Perform one of the following steps:

a If the Tree Trace parameter is not configured, go to step 6.

b If the Tree Trace parameter is configured, go to step 7.

6 Select Configured from the Tree Trace drop-down menu. The LDP Routing Instance (Edit) form re-opens with all parameters displayed.

7 Configure the tree discovery configuration parameters:

- Tree Trace
- Administrative State
- Discovery Interval (Minutes)
- Discovery Timeout (Seconds)
- Retry Count
- Maximum Paths
- Forwarding Class
- Profile
- Maximum TTL
- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5
- Probe Interval (Minutes)
- Probe Timeout (Minutes)
- Retry Count

8 Click on the Discovered FECs tab. A list of discovered FECs appears.

9 Choose a FEC from the list and click on the Properties button. An Autodiscovered FEC (Edit) form opens with the General tab displayed.

10 Perform one of the following:

a Click on the Create LDP Tree Trace button to configure and execute an LSP trace test. If the Create LDP Tree Trace button is not visible, click on the More Actions button and choose Create LDP Tree Trace. See chapter 32 for information about how to configure this test.

b Click on the Create LSP Ping button to configure and execute a LSP ping test. If the Create LSP Ping button is not visible, click on the More Actions button and choose Create LSP Ping. See chapter 32 for information about how to configure this test.

c Click on the Create LSP Trace button to configure and execute a LDP tree trace. If the Create LSP Trace button is not visible, click on the More Actions button and choose Create LSP Trace. See chapter 32 for information about how to configure this test.

11 Click on the Discovered ECMP tab. A list of ECMP paths associated with the FEC appears.

12 Choose an ECMP path from the list.

13 Click on the Properties button. An Autodiscovered Path (Edit) form opens.

14 Click on the Create LSP button. If the Create LSP button is not visible, click on the More Actions button and choose Create LSP. See chapter 32 for information about how to configure and execute an LSP trace test.

15 Click on the Create LSP Ping button. If the Create LSP Ping button is not visible, click on the More Actions button and choose Create LSP Ping. See chapter 32 for more information about how to configure and execute an LSP ping test.

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The Autodiscovered FEC (Edit) form closes.

Procedure 23-18 To view the LDP session information

Perform this procedure to check the status of and view the information about a LDP session.

1 Choose Routing from the navigation tree view selector.

2 Navigate to an LDP instance. The path is Routing→NE→Routing Instance→LDP.

3 Right-click on the LDP icon and choose Properties. The LDP - Routing Instance (Edit) form opens with the General tab displayed.

4 Click on the Sessions tab. A list of the active LDP sessions is displayed.

5 View the information.

6 To view the information for a specific session, choose the session entry and click on the Properties button. The Session (View) form opens with the General tab displayed.

7 Click on the Session tab to view specific session and connection information.

8 View information about the addresses exchanged in LDP peer sessions.

i Click on the Addresses tab. A list of the addresses received from peers is displayed on the Received tab.

ii To view the information about a received address, choose the address entry and click on the Properties button. The Received Addresses (View) form opens with the General tab displayed.

iii To view the information about the addresses sent to peers, click on the Sent tab. A list of the sent addresses is displayed.

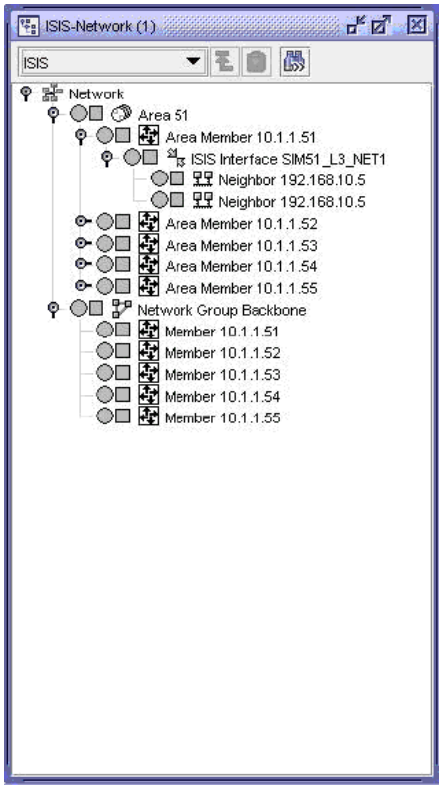
iv To view the information about a sent address, choose the address entry and click on the Properties button. The Sent Addresses (View) form opens with the General tab displayed.

9 Close the open forms, as required.

23.19 IS-IS configuration procedures

Configuration planning is essential to organize devices in level 1, level 2 and level 1 and 2 areas. IS-IS provides defaults for basic protocol operability. Use the 5620 SAM to configure the IS-IS parameters. Figure 23-7 shows the IS-IS view in the navigation tree

Figure 23-7 IS-IS view



The IS-IS information that is displayed includes:

- backbone area and backbone-area devices
- a list of areas and the participating routers in each area
- a list of devices and associated interfaces that shows the IP address and the configured level (1, 2, or 1 and 2) of each interface
- the IS-IS adjacencies for each interface

The following procedures describe how to configure IS-IS.

Procedure 23-19 To enable IS-IS on a routing instance

1 Choose Routing from the navigation tree view selector. The Routing view is displayed.

2 Expand the device object. The Routing Instance object is displayed.

3 Right-click on the routing instance icon and choose Properties. The Routing Instance (Edit) form opens.

4 Enable the IS-IS protocol.

  i Click on the Protocols tab.

  ii Select the IS-IS Enabled parameter.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. IS-IS is displayed in the list of enabled protocols.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The Routing Instance (Edit) form closes, and an ISIS Instance object is displayed in the navigation tree.

Procedure 23-20 To configure IS-IS on a routing instance

Routing instance IS-IS parameter values can differ from the IS-IS interface parameter values that are configured in Procedure 23-23. Interface capabilities are compared to the router-wide capabilities to determine the type of level 1, level 2, and level 1 and 2 adjacencies that are set up between routers to exchange IS-IS routing information.

1 Enable the IS-IS protocol on a routing instance, as described in Procedure 23-19.

2 Choose Routing from the navigation tree view selector. The Routing view is displayed.

3 Perform one of the following:

a Choose *NE*→Routing Instance→ISIS Instances to navigate to the ISIS Instances object (except 7705 SAR NEs).

b For 7705 SAR NEs, which display only one ISIS instance, navigate to the ISIS object and go to step 4 b ii.

4 Perform one of the following:

a Create an IS-IS instance.

i Right-click on the ISIS Instances object and choose Create ISIS Instance. The ISIS, Routing Instance, ISIS Instance (Create) form opens with the General tab displayed.

ii Configure the Instance ID parameter.

b Modify an IS-IS instance.

i Expand the ISIS Instances object.

ii Right-click on an ISIS Instance object and choose Properties from the contextual menu. The ISIS, Routing Instance, ISIS Instance (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Administrative State
- Level Capability

A level 1 adjacency can be established when there is at least one area ID shared by this router and a neighboring router. A level 2 adjacency is established when another router is configured as a level 2 or a level 1 and 2 router with interfaces configured as level 2 or level 1 and 2. A level 1 and 2 adjacency is created when the neighboring router is also configured as a level 1 and 2 router and the routers have at least one area ID in common.



Note — The available parameters vary, depending on the NE type.

6 Click on the Behavior tab.

7 Configure the parameters in the General panel:

- Traffic Engineering
- Unicast Import IPv4
- Unicast Import IPv6
- Multicast Import IPv4
- Multicast Import IPv6
- Hello Authentication
- CSNP Authentication
- PSNP Authentication
- Multi-Topology
- IPv6 Unicast Multi-Topology
- Enable LDP Synchronization
- LDP over RSVP Include
- Default Route Tag
- Suppress Default Routes
- Advertise Only Passive Interfaces
- RSVP Shortcut Enabled
- Advertise Tunnel Links Enabled
- Export Limit
- IID TLV
- Loop-free Alternate

You can only configure the IPv6 Unicast Multi-Topology parameter when the Multi-Topology parameter is set to true.



Note — If you plan to enable IPv6 on the IS-IS instance (see step 15), you must set the Multi-Topology and IPv6 Unicast Multi-Topology parameters to true.

8 Configure the Reference Bandwidth (Kb/s) parameter.

9 Configure the parameters in the Overload panel:

- Overload On Boot
- Overload On Boot Timeout (seconds)
- Overload
- Overload Timeout (seconds)

10 Configure the parameters in the Link State PDU panel:

- LSP Lifetime (seconds)
- LSP Max Wait (seconds)
- LSP Initial Wait (seconds)
- LSP Second Wait (seconds)
- LSP MTU Size

11 Configure the parameters in the Shortest Path First panel:

- SPF Max Wait (seconds)
- SPF Initial Wait (milliseconds)
- SPF Second Wait (milliseconds)

12 Click on the Graceful Restart tab.

13 Configure the parameters:

- Graceful Restart
- Helper Mode

14 Depending on the device type and configuration, the IP Versions tab is configurable. Click on the IP Versions tab to specify the allowed IP versions for the IS-IS instance.

15 Configure the parameters:

- Enable IPv6
- IPv6 Routing TLV type
- Enable IPv4
- Strict Adjacency Check

16 Click on the Authentication tab.

17 Configure the parameters:

- Enable Authentication
- Type
- Key

18 Click on the Level 1 tab.

19 Configure the parameters on the General sub-tab:

- External
- Internal
- Wide Metrics Only
- Hello Authentication
- CSNP Authentication
- PSNP Authentication
- Loop-free Alternate Exclude
- Default Metric
- IPv6 Default Metric

20 Click on the Authentication sub-tab.

21 Configure the parameters:

- Type
- Key

22 Click on the Level 2 tab.

23 Repeat steps 19 to 21.

24 Click on the Export Policies tab.

25 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

You can specify multiple routing policies, in order of preference, to determine the routes that are exported from the routing table to IS-IS. When multiple policies are specified, the policies are evaluated in numerical order.

26 Click on the NET addresses tab.

27 Click on the Create button.

28 Configure the Area ID parameter.

29 Click on the OK button. A dialog box appears.

30 Click on the OK button. The new NET address is displayed on the NET Addresses tab.

31 Click on the Route Summarizations tab. IS-IS route summaries allow users to create aggregate IPv4 or IPv6 addresses that include multiple groups of IPv4 or IPv6 addresses for a specific IS-IS summary level. This can help reduce the size of the link state database and the routing table.

32 Click on the Create button. The Route Summarization (Create) form opens.

33 Configure the parameters:

- Network
- Mask
- Summary Level
- Summary Route Tag

34 Click on the OK button. A dialog box appears.

35 Click on the OK button. The new route summary is displayed on the form.

36 Click on the Interfaces tab to add an IS-IS interface, if required.

i Click on the Create button. The ISIS Interface (Create) form opens, with the General tab displayed.

ii Click on the Select button. The Select Interface - IS-IS Interface form opens.

iii Configure the filter criteria, if required, and click on the Search button. A list of the available interfaces appears.

iv Choose an interface in the list and click on the OK button. The Select Interface - ISIS Interface form closes, and the interface information appears on the ISIS Interface (Create) form.

v Perform steps 5 to 15 of Procedure 23-23.

vi Click on the OK button. A dialog box appears.

vii Click on the OK button. The new interface is listed on the form.

37 Click on the OK button. A dialog box appears.

38 Click on the Yes button. The IS-IS (Edit) form closes.

Procedure 23-21 To configure an IS-IS link group on a routing instance

You can create an IS-IS link group to bundle multiple member interfaces that are treated as a single virtual link for ECMP. See Procedures 23-20 and 23-23 for more information about how to create and configure IS-IS interfaces.

1 Choose Routing from the navigation tree view selector. The Routing view is displayed.

2 Perform one of the following:

a Choose *NE*→Routing Instance→ISIS Instances to navigate to the ISIS Instances object (except 7705 SAR NEs).

b For the 7705 SAR, which displays only one ISIS instance, navigate to the ISIS object and go to step 3.

3 Expand the ISIS Instances object.

4 Right-click on an ISIS Instance object and choose Properties from the contextual menu. The ISIS Routing Instance, ISIS Instance (Edit) form opens with the General tab displayed.

5 Click on the Link Group tab.

6 Click on the Create button. The Link Group Config (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Group Name
- Description

8 Click on the OK button. A dialog box appears.

9 Click on the OK button. The Link Group Config (Create) form closes.

10 Click on the Apply button. A dialog box appears.

11 Click on the Yes button.

12 Choose the link group that you created and click on the Properties button. The Link Group Config (Edit) form opens with the General tab displayed.

13 Click on the Level 1 tab. The General tab is displayed.

14 Configure the parameters:

- Operational Members
- Revert Members
- IPv4 Unicast Metric Threshold
- IPv4 Multicast Metric Threshold
- IPv6 Unicast Metric Threshold
- IPv6 Multicast Metric Threshold

15 Click on the Members tab.

16 Click on the Add button. The Select... form opens.

17 Click on the Search button. A list of interfaces appears.

18 Choose an interface and click on the OK button. The Select... form closes.

19 Click on the Level 2 tab. The General tab is displayed.

20 Configure the parameters:

- Operational Members
- Revert Members
- IPv4 Unicast Metric Threshold
- IPv4 Multicast Metric Threshold
- IPv6 Unicast Metric Threshold
- IPv6 Multicast Metric Threshold

21 Click on the Members tab.

22 Click on the Add button. The Select... form opens.

23 Click on the Search button. A list of interfaces appears.

24 Choose an interface and click on the OK button. The Select... form closes.

25 Click on the OK button. A dialog box appears.

26 Click on the Yes button. The Link Group Config (Edit) form closes.

27 Close the ISIS Routing Instance, ISIS Instance (Edit)

Procedure 23-22 To configure an IS-IS NET address

1 Enable the IS-IS protocol on a device, as described in Procedure 23-19.

2 Choose Routing from the navigation tree view selector. The Routing view is displayed.

3 Perform one of the following:

a Choose *NE*→Routing Instance→ISIS Instances→ISIS Instance to navigate to the ISIS Instance object (except 7705 SAR NEs).

b For 7705 SAR NEs, which display only one IS-IS instance, navigate to the ISIS object.

4 Right-click on the ISIS Instance object and choose Add NET Address. The Area ID (Create) form opens.

5 Configure the Area ID parameter.



Note — The Area ID forms part of the NET address. NET addresses are built from some non-configurable elements, including the device system ID and the network selector ID.The NET address is exchanged in hello and link-state PDUs. Level 1 interfaces must have at least one area ID in common. Level 2 interfaces can have different area IDs. If all of the interfaces have different area IDs, they are considered level 2 interfaces only.

6 Click on the OK button. The Area ID (Create) form closes, and an icon for the new area appears in the navigation tree below the ISIS object.

Procedure 23-23 To configure an IS-IS interface

The IS-IS interface parameters can differ from the IS-IS routing instance parameters configured in Procedure 23-20. Interface parameters specify the interface routing levels. Interface level capabilities are compared to the router-wide level capabilities to determine the type of level 1, level 2, and level 1 and 2 adjacencies that are created between devices.

1 Enable the IS-IS protocol on a routing instance, as described in Procedure 23-19.

2 Choose Routing from the navigation tree view selector. The Routing view is displayed.

3 Perform one of the following:

- **a** Choose *NE*→Routing Instance→ISIS Instances →ISIS Instance to navigate to the ISIS Instance object (except 7705 SAR NEs). If no IS-IS instance exists, you must create one by performing Procedure 23-20.
- **b** For 7705 SAR NEs, which display only one IS-IS instance, navigate to the ISIS object.

4 Perform one of the following:

- **a** Create an IS-IS interface.
  - **i** Right-click on the ISIS Instance object and choose Create Interface. The ISIS Interface (Create) form opens with the General tab displayed.
  - **ii** Click on the Select button to choose a network interface. The Select Interface - IS-IS Interface form opens.

iii Configure the filter criteria, if required, and click on the Search button. A list of the available interfaces appears.

iv Choose an interface and click on the OK button. The Select Interface - ISIS Interface form closes, and the interface information appears on the ISIS Interface (Create) form.

b Modify an IS-IS interface.

i Expand the ISIS Instance object.

ii Right-click on an ISIS Interface object and choose Properties from the contextual menu. The ISIS Interface (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Description
- Administrative State
- Type
- Level Capability
- IPv4 BFD Enabled
- IPv6 BFD Enabled

6 Click on the Behavior tab.

7 Configure the parameters:

- CSNP Interval (seconds)
- LSP Pacing Interval (seconds)
- Retransmit Interval (seconds)
- Mesh Group Status
- Mesh Group
- Passive
- IPv6 Unicast Enabled
- Route Tag
- Loop-free Alternate Exclude

To create a mesh group, set the Mesh Group Status parameter to Enabled and specify the same mesh group value for all interfaces. The mesh group parameters specify the assigned mesh group for the interface. Mesh groups limit the amount of flooding that occurs when a new or changed LSP is advertised in an area.

The TE Metric parameter is a read-only field that displays the TE metric used for LSP path computation by CSPF.

8 Click on the Authentication tab.

9 Configure the parameters:

- Enable Authentication
- Type
- Key

10 Click on the Level 1 tab.

11 Configure the parameters on the General sub-tab:

- Hello Interval (seconds)
- Hello Multiplier
- Metric
- IPv6 Unicast Metric
- Passive
- Priority
- Signal Degrade Threshold
- Signal Fail Threshold

12 Click on the Authentication sub-tab.

13 Configure the parameters:

- Type
- Key

14 Click on the Level 2 tab.

15 Repeat steps 11 to 13.

16 Click on the OK button. The IS-IS Interface (Create) form closes, and the new interface is displayed in the navigation tree below the ISIS Instance icon.

23.20 OSPF configuration procedures

The 5620 SAM supports the configuration of OSPFv2 and OSPFv3.



Note 1 — The following devices support OSPFv3:

- 7450 ESS, in mixed mode
- 7710 SR
- 7750 SR, in chassis mode C or D
- 7750 SR, in chassis mode A or B, with mixed mode enabled
- 7950 XRS

Note 2 — The 7450 ESS, 7710 SR, 7750 SR, and 7950 XRS support multiple OSPFv2 and OSPFv3 instances on the base routing instance and on VPRN routing instances.

Note 3 — The following devices support only one OSPF instance on a VRF instance:

- OS 10K
- OS 6850E
- OS 6850E-U24X
- OS 6900
- OS 9700E
- OS 9800E

Note 4 — The 7450 ESS in mixed mode, the 7710 SR, the 7750 SR in chassis mode C or D, and the 7950 XRS support multiple OSPF instances in VPRN services.

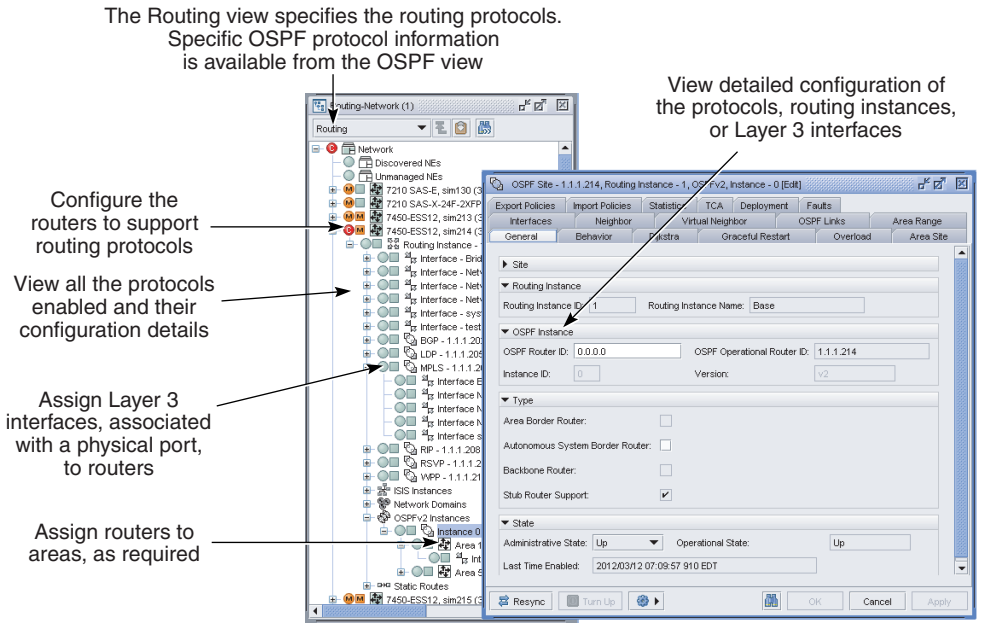
Note 5 — The 7210 SAS-M supports only one OSPF instance.

Configuration planning is essential to organize OSPF areas, interfaces, and virtual links. OSPF provides defaults for basic protocol operability. OSPF configuration requires, as a minimum, that:

- you create a single OSPF backbone area that contains the area border routers.
- for larger networks, you create several areas that contain the other routers.
- for smaller networks, you place all routers in the OSPF backbone area.

Use the 5620 SAM navigation tree to configure the OSPF parameters. Figure 23-8 shows the OSPF view in the navigation tree.

Figure 23-8 OSPF view



The OSPF parameters that are required for OSPF deployment are:

- Router ID — Each device that runs OSPF must be configured with a unique router ID. The router ID is used by the OSPF and BGP routing protocols in the routing table manager. When you configure a new router ID, protocols are not automatically restarted with the new router ID. You must shut down and restart the protocol to initialize the new router ID.
- An area — At least one OSPF area must be created. An interface must be assigned to each OSPF area. The types of OSPF areas include a backbone area, stub area, and NSSA.
- Layer 3 interfaces — A Layer 3 interface is the logical IP connection between a router and one of its attached networks. A physical interface is associated with the Layer 3 interface to provide the cabled connected to another device. A Layer 3 interface has state information from the underlying lower-level protocols and the routing protocol. A network interface has an associated IP address and mask that combine to create an IP prefix, unless the interface is in an unnumbered, point-to-point network.

The following procedures describe how to configure OSPF.

Procedure 23-24 To enable OSPF on a routing instance

1 Choose Routing from the navigation tree view selector from the 5620 SAM GUI.

2 Choose Routing→Router→Routing Instance.

3 Right-click on the routing instance icon and choose Properties. The Routing Instance (Edit) form opens.

4 Click on the Protocols tab.

5 Select the OSPFv2 Enabled parameter to enable OSPFv2, if required.

6 Select the OSPFv3 Enabled parameter to enable OSPFv3, if required.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The Routing Instance (Edit) form closes, and an icon for each newly enabled protocol appears under the routing instance in the navigation tree.

Procedure 23-25 To create an OSPF area

1 In the 5620 SAM navigation tree, choose OSPF from the view selector.

2 Right-click on the Network icon and choose Create Area from the contextual menu. The Area (Create) form opens.

3 Configure the parameters:

- Version
- Area ID
- Name
- Type
- Description

4 Click on the Apply button. The form refreshes with additional tabs.

5 Click on the Area Site tab.

6 Click on the Create button to add a routing instance to the area. The Area Site (Create) form opens with the General tab displayed.

7 Click on the Select button to choose a routing instance. The Select OSPF Instance - Area Site form opens.

8 Choose an OSPF instance and click on the OK button. The Select OSPF Instance form closes, and the OSPF instance appears in the Routing Instance panel.

9 Configure the parameters:

- Type
- Blackhole Range
- Loop-free Alternate Exclude

Configure the area as a blackhole range to avoid routing loops.

The Type parameter is not configurable for a backbone-area routing instance.

10 Click on the Apply button. Additional configurable tabs appear, and an icon for the new area appears in the navigation tree.

11 Depending on the Type parameter value, the Stub/NSSA tab is configurable. Configure stub or NSSA functionality, if required.

The Default Cost parameter is configurable only when the Type parameter value from step 9 is Stub (No Type 5 External) or Totally Stub (No Summaries).

i Click on the Stub/NSSA tab.

ii Configure the parameters:

- Default Cost
- Redistribute External Routes
- Originate Default Route
- Adjacency Check

The Redistribute External Routes, Originate Default Route, and Adjacency Check parameters are configurable only when the Type parameter value from step 9 is NSSA (No Type 5 External) or NSSA (No Summaries).

The Adjacency Check parameter is configurable only when the Originate Default Route is set to Originate Type 3 or Originate Type 7. Enable the Adjacency Check parameter to enforce an ABR to have an adjacency in area 0 before the default route or routes can be advertised into the NSSA.

12 If the area is a backbone area that requires links to remote areas that do not advertise OSPF topology, configure a virtual link.

i Click on the Virtual Link tab.

ii Perform steps 4 to 8 of Procedure 23-29.

iii Click on the OK button. The new virtual link entry appears in the list.

13 Create an area range, if required.

i Click on the Area Range tab.

ii Click on the Create button. The Area Range (Create) form opens.

iii Perform steps 5 and 6 of Procedure 23-28.

iv Click on the OK button. The new area range entry appears in the list.

14 Click on the OK button. The Area Site (Create) form closes, and a dialog box appears.

15 Click on the Yes button to confirm the action.

Procedure 23-26 To create an OSPF neighbor on an OmniSwitch

1 In the 5620 SAM navigation tree, choose Routing from the view selector.

2 Choose Routing→Router→Routing Instance→OSPFv2.

3 Right-click on the OSPFv2 Instance icon and choose Create Neighbor from the contextual menu. The OspfNeighbor (Create) form opens.

4 Configure the parameters:

- Neighbor IP Address
- Priority/Eligibility

5 Click on the OK button. The OspfNeighbor (Create) form closes.

Procedure 23-27 To add a Layer 3 interface to an OSPF router

Perform this procedure to allow an OSPF-enabled router to participate in area discovery and share routing information with other area members.



Note — This action assigns an existing Layer 3 interface to the router in the OSPF area rather than creating a new Layer 3 interface.

1 In the 5620 SAM navigation tree, choose OSPF from the view selector.

2 Click on an Area icon to display the area routers.

3 Right-click on a router instance icon and choose Create Interface. The OSPF Interface (Create) configuration form opens with the General tab displayed.

4 Configure the parameters:

- Description
- Administrative State
- Configured MTU (bytes)

5 Click on the Select button beside the Interface Name parameter to choose an interface. The Select Interface - OSPF Interface form opens.

6 Configure the filter criteria. A list of available Layer 3 interfaces appears.

7 Choose a Layer 3 interface and click on the OK button. The Select Interface - OSPF Interface form closes, and the interface entry appears in the Interface panel.

8 Click on the Protocol Properties tab.

9 Configure the parameters:

- Type
- Priority
- Metric
- Advertise Subnet
- BFD Enabled
- Loop-free Alternate Exclude
- LSA Filter Out
- Passive
- Hello Interval (seconds)
- Router Dead Interval (seconds)
- Retransmission Interval (seconds)
- Transit Delay (seconds)

The Advertise Subnet parameter is configurable for OSPFv2 only.

The TE Metric check box is a read-only field that indicates whether the TE Metric parameter is being configured in the interface for LSP path computation by CSPF.

10 Perform one of the following steps to configure authentication for the interface, if required. Otherwise, go to step 13.

a Click on the Authentication tab, and go to step 11.

b For OSPFv3 interfaces, click on the IPsec Static SA tab, and go to step 12.

11 Configure the Authentication Type parameter.

a Choose MD5-based Authentication.

i Click on the Create button to create an MD5 authentication key. The Md5Key (Create) form opens.

ii Configure the parameters:

- Key Index
- Key
- Re-enter Key

iii Click on the OK button. A dialog box appears.

iv Click on the Yes button. The Md5Key (Create) form closes, and the new authentication key appears in the list.

b Choose Simple Password.

i Click on the Change Password button to enter a password. The Password (Create) form opens.

ii Configure the parameters:

- Password
- Re-enter Password

iii Click on the OK button. A dialog box appears.

iv Click on the Yes button. The Password (Create) form closes.

12 Configure the parameters:

- IPsec Security Association Name
- IPsec In Static Security Association
- IPsec Out Static Security Association

13 Click on the OK button to close the OSPF Interface (Create) form. The 5620 SAM displays an icon for the new OSPF interface in the navigation tree below the area router.

Procedure 23-28 To create an OSPF area range

An area range summarizes a range of IP addresses in an LSA to minimize the number of flooded advertisements in the LSA.

1 In the 5620 SAM navigation tree, choose OSPF from the view selector.

2 Click on an Area icon in the navigation tree to display the area routers.

3 Expand the Router Instance icon.

4 Right-click on an Instance icon and choose Create Area Range. The Area Range (Create) form opens.

5 Configure the parameters:

- Network
- Prefix Length
- Link State DB Type
- Effect
- Metric

6 Click on the OK button. The Area Range (Create) form closes, and an icon for the new area range appears in the navigation tree below the OSPF area.

Procedure 23-29 To create a virtual link

Perform this procedure to create a virtual link between a backbone OSPF area and a remote OSPF area that does not advertise the OSPF topology. When you create a virtual link, a virtual neighbor is automatically created.

1 In the 5620 SAM navigation tree, choose OSPF from the view selector.

2 Click on the backbone area icon in the navigation tree to display the area routers. The backbone area ID is 0.0.0.0.

3 Right-click on a backbone-area router instance icon and choose Create Virtual Link. The Virtual Link (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Virtual Neighbor Router (Site) ID
- Transit Area

5 Click on the Protocol Properties tab.

6 Configure the parameters:

- Hello Interval (seconds)
- Router Dead Interval (seconds)
- Retransmission Interval (seconds)
- Transit Delay (seconds)

7 Perform one of the following steps to configure authentication for the virtual link, if required. Otherwise, go to step 10.

a Click on the Authentication tab, and go to step 8.

b For OSPFv3 interfaces, click on the IPsec Static SA tab, and go to step 9.

8 Configure the Authentication Type parameter.

a Choose MD5-based Authentication.

i Click on the Create button to create an MD5 authentication key. The Md5Key (Create) form opens.

ii Configure the parameters:

- Key Index
- Key
- Re-enter Key

iii Click on the OK button. A dialog box appears.

iv Click on the Yes button. The Md5Key (Create) form closes, and the new authentication key appears in the list.

v Go to step 10.

b Choose Simple Password.

i Click on the Change Password button to enter a password. The Password (Create) form opens.

ii Configure the parameters:

- Password
- Re-enter Password

iii Click on the OK button. A dialog box appears.

iv Click on the Yes button. The Password (Create) form closes.

v Go to step 10.

9 Configure the parameters:

- IPsec Security Association Name
- IPsec In Static Security Association
- IPsec Out Static Security Association

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The VirtualLink (Create) form closes, and the 5620 SAM displays two new icons: one for the virtual link and one for the virtual neighbor.

12 As required, review the properties of the virtual link or virtual neighbor, by clicking on the appropriate icon and selecting Properties from the contextual menu.



Note — You can delete a virtual link by selecting the virtual link icon and select delete from the contextual menu. To delete a virtual neighbor, you must select the virtual link icon and select delete from the contextual menu.

Procedure 23-30 To configure OSPF on a default routing instance or a VRF routing instance

1 In the 5620 SAM navigation tree, choose Routing from the view sector.

2 Perform one of the following:

- **a** For 7950 XRS, 7750 SR, 7450 ESS, and 7710 SR NEs, choose Network→Router→Routing Instance→OSPFv*N* Instances, where *N* is the OSPF version number; for example, 2 or 3.
- **b** For all other supported devices, choose Routing→Router→Routing Instance→OSPFv*N*, where *N* is the OSPF version number; for example, 2 or 3.

3 Perform one of the following:

- **a** For the 7950 XRS, 7750 SR, 7450 ESS, or 7710 SR, right-click on the appropriate OSPFv*N* Instances icon and choose Create OSPFv*N* Instance. The OSPF Site (Create) form opens with the General tab displayed. Go to step 4.
- **b** For all other supported devices, right-click on the appropriate OSPFv2 Instances icon and choose Properties. The OSPF Site, Routing instance, OSPFv2 instance (Edit) form appears. Go to step 4.

4 Configure the parameters:

- OSPF Router ID
- Instance ID
- Autonomous System Border Router
- Domain ID
- Administrative State

5 Click on the Behavior tab.

6 Configure the parameters:

- Traffic Engineering Support
- Interface Base Reference Cost (kbps)
- Overload Stubs
- Unicast Import
- Multicast Import
- Enable LDP Synchronization
- Ignore DN Bit
- Suppress DN Bit
- RFC1583 Compatible
- Loop-free Alternate
- LDP over RSVP Include
- Advertise Tunnel Links Enabled
- Exit Overflow Interval
- External LSA Limit
- Internal
- External

The Traffic Engineering Support, RFC1583 Compatible, LDP over RSVP Include, Multicast Import, and Unicast Import parameters are configurable for OSPFv2 only.

7 Click on the Dijkstra tab.

8 Configure the following parameters:

For SPF:

- SPF Max Wait (milliseconds)
- Redistribute Delay (milliseconds)
- Initial Wait (milliseconds)
- Second Wait (milliseconds)
- Incremental SPF Wait (milliseconds)

For LSA:

- LSA Generate Max Wait (milliseconds)
- LSA Arrival Wait (milliseconds)
- Initial Wait (milliseconds)
- Second Wait (milliseconds)
- LSA Accumulate (milliseconds)

9 Configure graceful restart, if required.

i Click on the Graceful Restart tab.

ii Configure the parameters:

- Graceful Restart
- Helper Mode

The Helper Mode parameter is configurable when the Graceful Restart parameter is set to true.

10 Depending on the OSPF version, the Overload tab is configurable. Configure overload, if required.

i Click on the Overload tab.

ii Configure the parameters:

- Overload Enabled
- Boot Overload Enabled
- Overload Interval (seconds)
- Boot Overload Interval (seconds)

The Overload Interval (seconds) parameter is configurable when the Overload Enabled parameter is selected.

The Boot Overload Interval (seconds) parameter is configurable when the Boot Overload Enabled parameter is enabled.

11 If the OSPF version is OSPFv2, the OSPF Super-Backbone tab is configurable. Configure the OSPF super-backbone, if required.

i Click on the OSPF Super-Backbone tab.

ii Configure the parameters:



Note — These parameters apply only to VPRN instances of OSPF.

- VPN Domain Type
- VPN Domain ID (hex)
- VPN Tag
- Super-Backbone

12 Click on the Export Policies tab to specify the export routing policies that determine the routes that are advertised to peers. Export policies are created as routing policy statements. See Procedure 22-15 for more information.

13 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

14 Click on the Import Policies tab to specify the import routing policies that determine the routes that are advertised to peers. Import policies are created as routing policy statements. See Procedure 22-15 for more information.

15 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

16 Click on the following tabs to add optional OSPF configuration items. Click on the Search button to list previously configured items or click on the Create button to create the item, if supported.

- Area Sites; see Procedure 23-25
- Interfaces (Layer 3 interfaces); see Procedure 23-27
- Area Range; see Procedure 23-28
- Virtual Neighbor; see Procedure 23-29
- OSPF Links (configurable only in a backbone area); see Procedure 23-29

Click on the remaining tab view additional OSPF configuration information, if required.

17 Click on the OK button. A dialog box appears.

18 Click on the Yes button to close the OSPF Site (Edit) form.

Procedure 23-31 To add a router to an OSPF area

1 In the 5620 SAM navigation tree, choose OSPF from the view selector.

2 Navigate to the OSPF area to which you want to add a router. The path is Routing→OSPF Area.

3 Right-click on the area icon and choose Add OSPF Instance. The Area Site (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Type
- Blackhole Range
- Loop-free Alternate Exclude

Configure the area as a blackhole range to avoid routing loops.

5 Click on the Select button below the Routing Instance panel to choose a routing instance. The Select OSPF Instance - Area Site form opens.

6 Choose a routing instance and click on the OK button. The routing instance appears in the Routing Instance panel.

7 Depending on the Type parameter value from step 4, the Stub/NSSA tab is configurable. Configure stub or NSSA functionality, if required.

i Click on the Stub/NSSA tab.

ii Configure the parameters:

- Default Cost
- Redistribute External Routes
- Originate Default Route
- Adjacency Type

The Default Cost parameter is configurable only when the Type parameter value from step 4 is Stub (No Type 5 External) or Totally Stub (No Summaries).

The Redistribute External Routes, Originate Default Route, and Adjacency Check parameters are configurable only when the Type parameter value from step 4 is NSSA (No Type 5 External) or NSSA (No Summaries).

The Adjacency Check parameter is configurable only when the Originate Default Route is set to Originate Type 3 or Originate Type 7. Enable the Adjacency Check parameter to enforce an ABR to have an adjacency in area 0 before the default route or routes can be advertised into the NSSA.

8 Click on the OK button. The Area Site (Create) form closes, and an icon for the router appears in the navigation tree under the OSPF Area icon.

23.21 RSVP configuration procedures

The following procedures describe how to configure RSVP.

Procedure 23-32 To configure RSVP on a routing instance

1 Navigate to an RSVP icon. The path is Routing→Router→Routing Instance→RSVP.

2 Right-click on the RSVP icon and choose Properties. The RSVP form opens with the General tab displayed.

3 Configure the parameters:

- Administrative State
- Keep Multiplier
- Refresh Time
- Message Pacing
- Enable Graceful Shutdown
- Enable Implicit Null Label
- Max Burst
- Period (milliseconds)
- Rapid Retransmit Time (hundred-milliseconds)
- Rapid Retry Limit
- Enable Refresh Bypass
- Soft Preemption Timer (seconds)

4 If you are going to configure Diff-Serv TE, then MPLS must be shutdown first. Otherwise, go to step 18.

5 Configure the parameters:



Note 1 — Enabling a Diff Serv Model only takes effect if you have already enabled traffic engineering at one or both of the following routing protocol levels:

- IS-IS, as described in Procedure 23-20
- OSPF, as described in Procedure 23-30

A dialog box appears if IS-IS and/or OSPF TE is not enabled, but you can save your configuration if IS-IS and/or OSPF TE is not enabled.

Note 2 — The Class Type BW Percent parameters are configured globally and the parameters are applied to all RSVP interfaces in the system. After the parameters are configured, the parameters can only be changed after you shut down the MPLS protocol. The total bandwidth specified for the eight classes should not exceed 100%.

- Diff Serv Model
- TE Threshold Update Enabled
- Class Type 0 BW Percent
- Class Type 1 BW Percent
- Class Type 2 BW Percent
- Class Type 3 BW Percent
- Class Type 4 BW Percent
- Class Type 5 BW Percent
- Class Type 6 BW Percent
- Class Type 7 BW Percent
- Update On CAC Failure Enabled
- Update Timer (seconds)

6 Configure the Include Node in RRO parameter.

7 Configure the parameters in the Merge Point Abort Timer panel:

- P2P Merge Point Abort Timer
- P2MP Merge Point Abort Timer

8 Configure the restart parameters in the GR Helper Time panel.

- Max Recovery Time (seconds)
- Max Restart Time (seconds)

9 Click on the TE Classes tab.

10 Select one of the TE classes in the table and click on the Properties button. The TE Class (Create) form opens.



Note — The TE Class Definition is used to map all TE Classes (up to a maximum of 8) to Class Type and LSP setup priority. There is no default TE Class after Diff-Serv is enabled. You must explicitly define each TE Class. If Diff-Serv is disabled, the default CT (CT0) and eight pre-emption priorities are used internally.

11 Configure the parameters:

- Priority
- TE Class Type

12 Click on the ForwardingClassMaps tab.

13 Click on the Create button. The Forwarding Class Map (Create) form opens.

14 Configure the parameters:

- FC Name
- TE Class Type

15 Repeat steps 10 to 14 for the remaining TE classes, as required.

16 Click on the TE Thresholds tab.

17 Configure the parameters:

- Up Threshold (%) (1 through 16)
- Down Threshold (%) (1 through 16)

You can also click the Reset TE Up/Down Thresholds to Default buttons to set the Up or Down Thresholds to their default values, respectively.

18 Click on the following tabs to view information.

- Interfaces
- Sessions
- Neighbors
- Statistics
- Faults

19 Click on the OK button. A dialog box appears.

20 Click on the Yes button. The RSVP form closes.

Procedure 23-33 To configure an RSVP interface

1 Navigate to an RSVP interface icon. The path is Routing→Router→Routing Instance→RSVP→Interfaces→Interface.

2 Right-click on the RSVP interface and choose Properties. The RSVP Interface (Edit) form opens with the General tab displayed.

3 Configure the parameters:

- Description
- Administrative State

4 Click on the Protocol Properties tab.

5 Configure the parameters:

- Enable Refresh Reduction
- Enable Reliable Delivery
- Enable Graceful Shutdown
- Enable Implicit Null Label
- Hello Interval (milliseconds)
- Subscription Ratio
- BFD Enabled
- Graceful Restart Helper Mode
- Inherit SAM Class Type BW
- Class Type 0 BW Percent
- Class Type 1 BW Percent
- Class Type 2 BW Percent
- Class Type 3 BW Percent
- Class Type 4 BW Percent
- Class Type 5 BW Percent
- Class Type 6 BW Percent
- Class Type 7 BW Percent

The Class Type BW Percent parameters can only be configured if the Inherit SAM Class Type BW parameter is disabled. If you enter values at the RSVP interface level, they override the global values configured in Procedure 23-32 for the RSVP routing instance on the NE.

6 Click on the Authentication tab.

7 Configure the Key parameter.

8 Click on the TE Thresholds tab.

9 Configure the parameters:

- Inherit TE Up Thresholds
- Inherit TE Down Thresholds
- Up Threshold (%) (1 through 16)
- Down Threshold (%) (1 through 16)

You can only configure the Up Threshold (%) and Down Threshold (%) parameters if the Inherit TE Up Thresholds and Inherit TE Down Thresholds parameters are disabled, respectively.

10 Click on the following tabs to view information.

- Neighbors
- Statistics
- Faults

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The RSVP Interface (Edit) form closes.

23.22 L2TP configuration procedures

The 5620 SAM supports the configuration and management of L2TP sites, tunnel group profiles, and tunnel profiles.

A typical L2TP configuration is applied to two NEs; one NE performs the LAC role and the other NE performs the LNS role. An NE can perform both LAC and LNS roles. At least one ISA-LNS group must be configured for the LNS NE. See section 14.5 for information about ISA-LNS groups. See Procedure 14-6 for information about creating and configuring an ISA-LNS group member.

Note 1 — An NE must be in chassis mode B or higher to support L2TP.

Note 2 — You can also enable L2TP on a VPRN site. See chapter 71 for more information.

The following procedures describe how to configure L2TP.

Procedure 23-34 To configure L2TP on a routing instance

Note 1 — For most parameters in this procedure, you can specify that the parameter value is inherited from the parent L2TP configuration using the Inherit Value parameter.

If you disable value inheritance for a parameter, the available options are restricted, based on the parent parameter value and the protocol functionality. For example, if a parameter in the global-level L2TP configuration is set to True, the only available option for the same parameter in the tunnel group profile-level L2TP configuration is False, unless a value of False violates a protocol rule, in which case the only available option is True.

Note 2 — The parameters that you configure for a L2TP tunnel group profile take precedence over the parameters that are configured for global-level L2TP.

1 Navigate to an L2TP icon. The path is Routing→Router→Routing Instance→L2TP.

2 Right-click on the L2TP icon and choose Properties. The L2TP Site (Edit) form opens with the General tab displayed.

3 Configure the parameters:

- Administrative State
- AVP Hiding
- Calling Number Format
- Challenge
- Cisco NAS-Port Ethernet
- Cisco NAS-Port ATM
- Destruct Timeout
- Excluded AVPs
- Group Session Limit
- Hello Interval
- Idle Timeout
- Local IP Address
- Local Name
- Max Retries Established
- Max Retries Not Established
- Next Attempt
- Password
- Peer Address Change Policy
- Receive Window Size
- Replace Result Code
- Session Assign Method
- Session Limit
- Tunnel Session Limit

4 Click on the Select button next to the RADIUS Accounting Policy field. The Select L2TP Accounting Policy form opens.

5 Choose an L2TP Accounting Policy from the list and click on the OK button. The Select L2TP Accounting Policy form closes and the RADIUS Accounting Policy field shows the displayed name of the selected accounting policy. Refer to Procedure 49-3 for information on creating an L2TP RADIUS Accounting Policy.

6 If required, click on the Tunnel Selection Blacklist tab and configure the parameters:

- Add Tunnel on
- Max List Length
- Max Time
- Timeout Action

7 Click on the Tunnel Group Profiles tab.

i Click on the Create button. The L2TP Tunnel Group Profile (Create) form opens with the General tab displayed.

ii Configure the parameters:

- Group Name
- Description
- Administrative State
- Local IP Address
- Local Name
- Password
- Challenge
- AVP Hiding
- Session Limit
- Session Assign Method
- Max Retries Established
- Max Retries Not Established
- Receive Window Size
- Hello Interval (seconds)
- Idle Timeout (seconds)
- Destruct Timeout (seconds)
- Load Balance Method



Note — To generate operational L2TP tunnels, a start operation must be performed on the L2TP tunnel on the LAC NE. You can also perform a start operation from a tunnel profile on the LNS.

8 Click on the Select button in the LNS Group ID panel and choose an LNS group from the Select LNS Group ID form.



Note — You must choose an LNS group for the tunnel group profile or tunnel profile of the site that acts as the LNS.

9 Click on the Select button in the L2TP Radius Accounting Policy panel and choose a RADIUS accounting policy from the Select L2TP RADIUS Accounting Policy form.

10 Configure PPP on the L2TP tunnel group profile, as required.



Note — PPP is required only for LNS L2TP tunnel group profiles and L2TP tunnel profiles.

i Click on the PPP tab.

ii Configure the parameters:

- Authentication Protocol
- Proxy LCP
- Proxy Authentication
- MTU (bytes)
- Keep-Alive Interval
- Keep-Alive Multiplier
- IPCP Subnet Negotiation
- LCP Ignore Magic Number

iii Configure the CHAP challenge length parameters, as required:

- Min
- Max

iv Configure an authentication policy, as required.

Click on the Select button in the Authentication Policy panel and choose an authentication policy from the Select Authentication Policy (PPPGroupProfile) form.

v If you did not choose an authentication policy in step iv, select a user database.

Click on the Select button in the User Database panel and choose a user database from the Select User Database (PPPGroupProfile) form.

vi Click on the Select button in the Default Service ID panel and choose a default service ID from the Select Default Service ID (PPPGroupProfile) form.

vii Click on the Select button in the Default Group Interface panel and choose a default group interface from the Select Default Group Interface (PPPGroupProfile) form.

11 Click on the Tunnel Profiles tab.

i Click on the Create button. The L2TP Tunnel Profile (Create) form opens with the General tab displayed.

ii Configure the parameters:

- Tunnel Name
- Description
- Administrative State
- Local IP Address
- Local Name
- Peer IP Address
- Remote Name
- Password
- Auto Established
- Preference
- Challenge
- AVP Hiding
- Session Limit
- Max Retries Established
- Max Retries Not Established
- Receive Window Size
- Hello Interval (seconds)
- Idle Timeout (seconds)
- Destruct Timeout (seconds)
- Load Balance Method



Note — When you configure parameters with the same name in a tunnel group profile and a tunnel profile, a non-default value in the tunnel group profile overrides the value specified for the L2TP site. Also, a non-default value in a tunnel profile overrides the value defined in the associated tunnel group profile and L2TP site.

iii As required, click on the Select button in the LNS Group ID panel and choose an LNS group from the Select LNS Group ID form.



Note — You must choose an LNS group for the tunnel group profile or tunnel profile of the site that acts as the LNS.

iv Click on the Select button in the L2TP Radius Accounting Policy panel and choose a RADIUS accounting policy from the Select L2TP RADIUS Accounting Policy form.

v Click on the PPP tab and repeat step 10 to configure PPP on the L2TP tunnel profile, as required.



Note 1 — You only configure PPP for LNS L2TP tunnel group profiles and L2TP tunnel profiles.

Note 2 — The values for the MTU, Keep-Alive Interval, Keep-Alive Multiplier, and CHAP Challenge Length Min and Max parameters can be inherited from the parent tunnel group profile.

vi Click on the MLPPP tab.

vii Configure the parameters:



Note — When Inherit from Tunnel Group Profile beside a parameter is enabled, the parameter value from the tunnel group profile is used. You must disable Inherit from Tunnel Group Profile beside a parameter before you can configure the parameter.

- Endpoint ID
- IPv4 Address
- MAC Address
- Interleave
- Max Fragment Delay
- Max MLPPP Links
- Reassembly Timeout
- Send Short Sequence Numbers
- Administrative State

viii Click on the OK button. A dialog box appears.

ix Click on the Yes button. The L2TP Tunnel Profile (Create) form closes.

12 Click on the MLPPP tab.

13 Configure the parameters:



Note — When Inherit from Tunnel Group Profile beside a parameter is enabled, the parameter value from the tunnel group profile is used. You must disable Inherit from Tunnel Group Profile beside a parameter before you can configure the parameter.

- Endpoint ID
- IPv4 Address
- MAC Address
- Interleave
- Max Fragment Delay
- Max MLPPP Links
- Reassembly Timeout
- Send Short Sequence Numbers
- Administrative State

14 Click on the OK button. A dialog box appears.

15 Click on the OK button. The L2TP Tunnel Group Profile (Create) form closes.

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The L2TP Site (Edit) form closes.

Procedure 23-35 To view L2TP tunnels and tunnel endpoints

1 Choose Manage→ISA Functions→ISA-L2TP from the 5620 SAM main menu. The Manage ISA-L2TP form opens.

2 Choose L2TP tunnel (L2TP) from the object drop-down menu.

3 Click on the Search button. A list of L2TP tunnels is displayed.

4 Choose an entry in the list and click on the Properties button. The L2TP Tunnel - Endpoint A - Endpoint B form opens with the General tab displayed.

5 View the information for Tunnel Endpoint A and Tunnel Endpoint B.

6 Click on the L2TP Tunnel Endpoints tab. The two L2TP tunnel endpoints are displayed.

7 Choose an entry in the list and click on the Properties button. The L2TP Tunnel Endpoint (View) form opens.

8 View the information. You can also click on the Properties button to view additional information for the following:

- Site ID
- Tunnel Instance Endpoint
- Tunnel Profile
- Tunnel Group Profile
- Peer

9 Close the L2TP Tunnel Endpoint (View) form.

10 Close the L2TP Tunnel - Endpoint A - Endpoint B form.

Procedure 23-36 To view L2TP tunnel instance endpoints on a subscriber instance

Perform this procedure to view L2TP tunnel instance endpoints associated with a specific subscriber instance.

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Residential Subscriber Instance (Residential Subscriber) from the object drop-down menu.

3 Configure the filter criteria, as required, and click on the Search button.

4 Choose a residential subscriber instance in the list and click on the Properties button. The Residential Subscriber Instance (Edit) form opens with the General tab displayed.

5 Click on the L2TP Tunnel Instance Endpoints tab.

6 Configure the filter criteria, as required, and click on the Search button. A dialog box opens.

7 Click on the Yes button.

8 Choose an L2TP tunnel instance endpoint in the list and click on the Properties button. The L2TP Tunnel Instance Endpoint (View) form opens with the General tab displayed.

9 View the information, as required. You can also click on the Sessions tab to view session information, as required.

10 Close the L2TP Tunnel Instance Endpoint (View) form.

11 Close the Residential Subscriber Instance (Edit) form.

12 Close the Manage Residential Subscribers form.

Procedure 23-37 To view L2TP sessions

Perform this procedure to view L2TP sessions on an L2TP site.

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose L2TP Session (L2TP) from the object drop-down menu.

3 Click on the Select button for the Site ID to choose a site.

4 Click on the Select button for the Routing Instance ID to choose a routing instance.

5 Configure the filter criteria, as required, and click on the Search button.

6 Choose a session in the list and click on the Properties button. The L2TP Session (View) form opens.

7 View the information in the following panels:

- Session
- Tunnel
- Operational Information
- LNS PPP



Note — The LNS PPP panel is applicable only for an LNS.

8 Close the L2TP Session (View) form.

9 Close the Manage Residential Subscribers form.

Procedure 23-38 To view PPP sessions

Perform this procedure to view PPP sessions.

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose PPP Session (PPP Policy and Session) from the object drop-down menu.

3 Click on the Select button for the Site ID to choose a site.

4 Click on the Select button for the Service ID to choose a service.

5 Configure the filter criteria, as required, and click on the Search button.

6 Choose a session in the list and click on the Properties button. The PPP Session form opens with the General tab displayed.

7 View the information in the following panels:

- PPP General
- Residential Subscriber
- Business Subscriber
- DHCP

8 Click on the following tabs to view the information, as required:

- Authentication Protocols
- DNS and NBNS IP Addresses
- QoS Overrides
- Deployment

9 Close the PPP Session form.

10 Close the Manage Residential Subscribers form.

23.23 PIM configuration procedures

The following procedures describe how to configure PIM.

Procedure 23-39 To enable PIM on a routing instance

1 Choose Routing from the navigation tree view selector.

2 Navigate to the routing instance icon. The path is Routing→Router→Routing Instance.

3 Right-click on the routing instance object and choose Properties. The Routing Instance (Edit) form opens with the General tab displayed.

4 Enable PIM:

i Click on the Multicast tab.

ii Select the PIM Enabled parameter.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Routing Instance (Edit) form closes, and a PIM icon appears in the navigation tree below the routing instance.

Procedure 23-40 To configure PIM on a routing instance



Note — If you are creating a PIM site on a VPRN routing instance, perform Procedure 23-41. See Procedure 71-50 for more information about configuring PIM on a VPRN routing instance.

1 Choose Routing from the navigation tree view selector.

2 Navigate to a PIM icon. The path is Routing→Router→Routing Instance→PIM.

3 Right-click on the PIM icon and choose Properties. The PIM Site (Edit) form opens with the General tab displayed.

4 Configure the Administrative State parameter in the States panel.

5 Configure the parameters in the PIM General Configurations panel:

- Apply To
- Non DR Attract Traffic
- RPF Vectors
- SSM Assert Compatible Mode
- Multicast Fast-failover

6 Configure the following parameters in the ECMP Balancing panel:

- ECMP Balancing Enabled
- Hold Time (minutes)
- ECMP Hashing Enabled

7 In the Lag Usage panel, configure the Lag Usage Optimization parameter.

8 Click on the RP Behavior tab. The IPv4 tab is displayed

9 If you are configuring for IPv4, click on the IPv4 tab and go to step 10. Otherwise click on the IPv6 tab and go to step 15.

10 Configure the IPv4 Administrative State parameter in the States panel.

11 Configure the following parameters in the PIM General Configurations panel:

- IPv4 RPF Lookup Sequence
- Auto RP Discovery Enabled

12 Configure the following parameters in the Candidate Bootstrap Router panel:

- CBSR Admin State
- CBSR Address
- CBSR Priority
- CBSR Hash Mask Length

13 Configure the following parameters in the Candidate Rendezvous Point panel:

- Administrative State
- C-RP Address
- C-RP Priority
- C-RP Hold Time (seconds)

14 Go to step 20.

15 Configure the IPv6 Administrative State parameter in the States panel.

16 Configure the IPv6 RPF Lookup Sequence parameter in the PIM General Configurations panel.

17 Configure the following parameters in the Candidate Bootstrap Router panel:

- CBSR Admin State
- CBSR Address
- CBSR Priority
- CBSR Hash Mask Length

18 Configure the following parameters in the Candidate Rendezvous Point panel:

- Administrative State
- C-RP Address
- C-RP Priority
- C-RP Hold Time (seconds)

19 Configure the following parameters in the Embedded-RP panel:

- Enable Embedded-RP
- Embedded-RP Administrative State

20 Add one or more C-RP groups, if required.

i Click on the Candidate-RP Groups tab.

ii Click on the Create button to add a new entry, if required. The C-RP Group Prefix (Create) form opens.

iii Configure the parameters:

- Group IP Address
- Mask

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The C-RP Group Prefix (Create) form closes and the new Candidate-RP entry appears in the table.

21 Add one or more embedded RP groups, if required.



Note — The Embedded-RP Groups tab is only selectable if you enabled the Enable Embedded-RP parameter in step 19.

i Click on the Embedded-RP Groups tab.

ii Click on the Create button to add a new entry, if required. The E-RP Group Range (Create) form opens.

iii Configure the parameters:

- Group IP Address
- Prefix

iv Click on the OK button. The E-RP Group Range (Create) form closes and the new Embedded-RP entry appears in the table.

22 Click on the Group To RP tab. The Static RP tab is displayed.

23 In the Static RP tab, click on the Create button to add a new entry, if required. The Static RP (Create) form opens.

24 Configure the parameters:

- Static RP IP Address
- RP Override

25 Click on the Static Group-To-RP tab.

26 Click on the Create button to add a new entry, if required. The Static Group To RP (Create) form opens.

27 Configure the parameters:

- Static Group IP Address
- Static Group Mask

28 Click on the OK button. A dialog box appears.

29 Click on the OK button. The new Static Group-To-RP entry appears on the form.

30 Click on the OK button. A dialog box appears.

31 Click on the OK button. The new Static RP entry appears on the form.

32 Click on the Import Policies tab.

33 Click on the BootStrap Import Policies tab.

34 Configure the parameters to filter bootstrap messages and to control the flow of bootstrap messages to the routing instance.

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

35 Click on the Join/Prune Import Policies tab.

36 Configure the parameters to filter join/prune messages.

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

37 Click on the Register Import Policies tab.

38 Configure the parameters to filter PIM register messages.

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

39 Click on the Export Policies tab.

40 Click on the BootStrap Export Policies tab.

41 Configure the parameters to filter PIM-related export messages.

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

42 Depending on the device release, the Anycast RP tab is configurable. Click on the Anycast RP tab to configure Anycast RP, if required.



Note — You can use the PIM configuration form to add peers to an anycast RP. The complete configuration of anycast RP for PIM requires additional supporting components, such as the configuration of loopback interfaces and static RPs. Due to the complex configuration dependencies, Alcatel-Lucent recommends that you use the Virtual Anycast manager. The Virtual Anycast manager automatically configures many of the supporting requirements for the protocol, which reduces operator configuration errors and assists in troubleshooting activities. See Procedure 23-42 for more information about using the Virtual Anycast manager.

43 Click on the General tab.

44 Configure the RP IP Address parameter.

45 Click on the Anycast Peer tab.

46 Click on the Create button to create a new entry, if required. The Anycast Peer (Create) form opens.

47 Configure the Peer IP Address parameter.

48 Click on the OK button. A dialog box appears.

49 Click on the OK button. The new anycast peer entry appears on the form.

50 Click on the OK button. A dialog box appears.

51 Click on the OK button. The new anycast RP entry appears on the form.

52 Click on the SSM Groups tab.

53 Click on the Create button to create a new entry, if required.

54 Configure the parameters:

- SSM Group IP Address
- SSM Group Mask

  The parameters are applicable to both IPv4 and IPv6.

55 Click on the OK button. A dialog box appears.

56 Click on the OK button. The new SSM group entry appears on the form.

57 Click on the Interfaces tab to create an interface, if required.

i Click on the Create button to add a new entry.

ii Perform steps 2 to 8 of Procedure 23-43.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The new interface entry appears on the form.

58 Click on the SPT Switch Threshold tab to configure SPT switchover, if required.

59 Click on the Create button to create a new entry, if required. The Spt Switch Over Threshold (Create) form opens.

60 Configure the parameters:

- Group IP Address
- Group Prefix Length
- Infinity For Threshold
- Threshold (kbps)

61 Click on the OK button. A dialog box appears.

62 Click on the OK button. The new SPT switch threshold entry appears on the form.

63 Click on the following tabs to view and edit information.

- Groups
- Neighbor
- Statistics
- Faults

The Statistics and Faults tabs are unavailable for PIM in VPRN.

64 Click on the OK button. A dialog box appears.

65 Click on the Yes button. The PIM (Edit) form closes.

Procedure 23-41 To create a PIM site on a VPRN routing instance

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service.

4 Click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

5 On the navigation tree, expand the Sites icon.

6 Expand the Routing Instance - NE System ID icon of the site to which you need to add the routing instance.

7 Expand the Routing Instance icon.

8 Right-click on the Protocols icon and choose Create PIM Site from the contextual menu. The PIM Site (Create) form opens with the General tab displayed.

9 Configure the Administrative State parameter in the States panel.

10 Configure the parameters in the PIM General Configurations panel:

- Apply To
- Non DR Attract Traffic
- SSM Assert Compatible Mode

11 Configure the following parameters in the ECMP Balancing panel:

- ECMP Balancing Enabled
- Hold Time (minutes)
- ECMP Hashing Enabled

12 Click on the RP Behavior tab. The IPv4 tab is displayed

13 If you are configuring for IPv4, click on the IPv4 tab and go to step 24. Otherwise click on the IPv6 tab and go to step 19.

14 Configure the IPv4 Administrative State parameter in the States panel.

15 Configure the following parameters in the PIM General Configurations panel:

- IPv4 RPF Lookup Sequence
- IPv4 SSM Default Range Disabled

16 Configure the following parameters in the Candidate Bootstrap Router panel:

- CBSR Admin State
- CBSR Address
- CBSR Priority
- CBSR Hash Mask Length

17 Configure the following parameters in the Candidate Rendezvous Point panel:

- Administrative State
- C-RP Address
- C-RP Priority
- C-RP Hold Time (seconds)

18 Go to step 24.

19 Configure the IPv6 Administrative State parameter in the States panel.

20 Configure the IPv6 RPF Lookup Sequence parameter in the PIM General Configurations panel.

21 Configure the following parameters in the Candidate Bootstrap Router panel:

- CBSR Admin State
- CBSR Address
- CBSR Priority
- CBSR Hash Mask Length

22 Configure the following parameters in the Candidate Rendezvous Point panel:

- Administrative State
- C-RP Address
- C-RP Priority
- C-RP Hold Time (seconds)

23 Configure the following parameters in the Embedded-RP panel:

- Enable Embedded-RP
- Embedded-RP Administrative State

24 Click on the MVPN tab. The General tab is displayed.

25 Configure the parameters:

- Auto-Discovery
- MCast Signaling
- Inclusive Tunnel Type
- Selective Tunnel Type
- US Multicast Hop Selection
- Inter-Site Shared
- MDT Type



Note — You must set the Inclusive Tunnel Type parameter to PIM, RSVP, or MLDP if you are creating an inclusive tunnel.

26 Click on the UMH PE Backup tab to configure primary and standby UMH addresses, if required.

i Click on the Create button. The MVPN UMH PE Backup (Create) form opens.

ii Configure the parameters:

- UMH Primary PE Address
- UMH Standby PE Address

iii Click on the OK button. The MVPN UMH PE Backup (Create) form closes and the new entry appears in the list.

27 Click on the MVPN Inclusive Tunnel tab.



Note 1 — The MVPN Inclusive Tunnel tab appears only if you set the Inclusive Tunnel Type parameter to an option other than None in step 25.

Note 2 — The tab that appears on the MVPN Inclusive Tunnel tab depends on the Inclusive Tunnel Type parameter option that you configured in step 25.

28 Perform one of the following:

a Create a PIM inclusive tunnel.

i Click on the PIM tab.

ii Configure the parameters:

- Provider Tunnel Inclusive PIM Mode
- Group Address

  The Group Address parameter is configurable if the Provider Tunnel Inclusive PIM Mode parameter is set to ASM or SSM.

iii Go to step 29.

b Create an RSVP inclusive tunnel.

i Click on the RSVP tab.

ii Configure the P2MP Administrative State parameter. You cannot set the P2MP Administrative State parameter to Up until you choose an MVPN LSP template. To create an MVPN LSP template, see Procedure 25-23.

iii Click on the Select button. The Select MVPN Lsp Template - RSVP MVPN Provider Tunnel form opens.

iv Choose an MVPN LSP template from the list and click on the OK button. The MVPN LSP template is displayed.

v Configure the parameters:

- Tunnel Root Enable BFD
- Tunnel Root BFD Transmit Interval
- Tunnel Root BFD Multiplier
- Tunnel Leaf Enable BFD

The Tunnel Root BFD Transmit Interval and Tunnel Root BFD Multiplier parameters are configurable when you enable the Tunnel Root Enable BFD parameter.

c Create an MLDP inclusive tunnel.

i Click on the MLDP tab.

ii Configure the P2MP Administrative State parameter.

iii Go to step 29.

29 Click on the MVPN Selective Tunnel tab. The General tab is displayed.

30 Configure the Delay Interval (seconds) parameter in the Data MDT panel.

31 Perform one of the following:

a Choose an existing data MVPN threshold entry.

i Click on the Search button in the Data MVPN Threshold tab.

ii Choose a Data MVPN Threshold entry from the list.

iii Click on the Apply button.

iv Go to step 32.

b Create and choose a data MVPN threshold entry.

i Click on the Create button in the Data MVPN Threshold tab. The Data MVPN Threshold (Create) form is displayed.

ii Configure the parameters:

- Group IP Address
- Group Prefix Length
- Threshold (kbps)

iii Click on the OK button. The Data MVPN Threshold (Create) form closes and the entry is displayed in the list.

iv Choose the Data MVPN Threshold entry that you created.

v Click on the Apply button.

32 Perform one of the following, if required:



Note — A data Multicast Tunnel (MT) is a connector between a set of PE routers forming a multicast domain. In the context of a VPN-specific PIM instance, a multicast tunnel is a single multi-access interface. The data MT Interface can be created or selected when the PIM address is configured with a value other than null (0.0.0.0).

a Choose an existing data MT interface entry.

i Click on the Search button in the Data MT Interface tab.

ii Choose a Data MT Interface entry from the list.

iii Click on the Apply button.

iv Go to step 33.

b Create and choose a data MT interface.

i Click on the Add button in the Data MT Interface tab. The Data MT Interface (Create) form is displayed.

ii Configure the parameters:

- Administrative State
- Hello Interval (seconds)
- Hello Multiplier
- Improved assert
- Three Way Hello
- Tracking Support

iii Click on the OK button. The Data MT Interface (Create) form closes and the entry is displayed in the list.

iv Choose the data MT interface that you created.

v Click on the Apply button.

33 Click on the PIM tab and configure the parameters:

- PIM Prefix
- PIM Prefix Length
- PIM Group Address Mode
- Pack Data Join TLV
- Auto-Discovery
- Enable ASM Data MDT

34 Click on the RSVP tab and configure the parameters:

- P2MP Maximum Spmsi
- P2MP Administrative State

The P2MP Maximum Spmsi parameter can be disabled by selecting the associated Disabled checkbox.

35 Click on the Select button in the RSVP panel to choose an MVPN Lsp Template. The Select MVPN Lsp Template form is displayed.

36 Perform one of the following:

a Choose an existing LSP template for MVPN.

i Click the Search button. All of the available MVPN p2mp LSP templates for the local NE (the NE contains this VPRN/PIM) are displayed.

ii Choose the required template and click on the OK button.

iii Go to step 37.

b Create an LSP template for MVPN.

i Click the Create button and perform Procedure 25-23.

ii Choose the newly-created template from the list in the Select MVPN Lsp Template form and click on the OK button.

37 The Select MVPN Lsp Template form closes and the RSVP tab is refreshed.

38 Click on the MLDP tab and configure the parameters:

- P2MP Maximum Spmsi
- P2MP Administrative State

The P2MP Maximum Spmsi parameter can be disabled by selecting the associated Disabled checkbox.

39 Click on the Import Policies tab.

40 Click on the BootStrap Import Policies tab.

41 Configure the parameters to filter bootstrap messages and to control the flow of bootstrap messages to the routing instance.

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

42 Click on the Join/Prune Import Policies tab.

43 Configure the parameters to filter join/prune messages.

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

44 Click on the Register Import Policies tab.

45 Configure the parameters to filter PIM register messages.

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

46 Click on the Export Policies tab.

47 Click on the BootStrap Export Policies tab.

48 Configure the parameters to filter PIM-related export messages.

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

49 Click on the Interfaces tab to create an interface, if required.

i Click on the Create button to add a new entry.

ii Perform steps 2 to 8 of Procedure 23-43.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The new interface entry appears on the form.

50 Add one or more C-RP groups, if required.

i Click on the Candidate-RP Groups tab.

ii Click on the Create button to add a new entry, if required. The C-RP Group Prefix (Create) form opens.

iii Configure the parameters:

- Group IP Address
- Mask

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The C-RP Group Prefix (Create) form closes and the new Candidate-RP entry appears in the table.

51 Click on the Group To RP tab. The Static RP tab is displayed.

52 In the Static RP tab, click on the Create button to add a new entry, if required. The Static RP (Create) form opens.

53 Configure the parameters:

- Static RP IP Address
- RP Override

54 Click on the Static Group-To-RP tab.

55 Click on the Create button to add a new entry, if required. The Static Group To RP (Create) form opens.

56 Configure the parameters:

- Static Group IP Address
- Static Group Mask

57 Click on the OK button. A dialog box appears.

58 Click on the OK button. The new Static Group-To-RP entry appears on the form.

59 Click on the OK button. A dialog box appears.

60 Click on the OK button. The new Static RP entry appears on the form.

61 Click on the SSM Groups tab.

62 Click on the Create button to create a new entry, if required.

63 Configure the parameters:

- SSM Group IP Address
- SSM Group Mask

  The parameters are applicable to both IPv4 and IPv6.

64 Click on the OK button. A dialog box appears.

65 Click on the OK button. The new SSM group entry appears on the form.

66 Click on the SPT Switch Threshold tab to configure SPT switchover, if required.

67 Click on the Create button to create a new entry, if required. The Spt Switch Over Threshold (Create) form opens.

68 Configure the parameters:

- Group IP Address
- Group Prefix Length
- Infinity For Threshold
- Threshold (kbps)

69 Click on the OK button. A dialog box appears.

70 Click on the OK button. The new SPT switch threshold entry appears on the form.

71 Depending on the device release, the Anycast RP tab is configurable. Click on the Anycast RP tab to configure Anycast RP, if required.



Note — You can use the PIM configuration form to add peers to an anycast RP. The complete configuration of anycast RP for PIM requires additional supporting components, such as the configuration of loopback interfaces and static RPs. Due to the complex configuration dependencies, Alcatel-Lucent recommends that you use the Virtual Anycast manager. The Virtual Anycast manager automatically configures many of the supporting requirements for the protocol, which reduces operator configuration errors and assists in troubleshooting activities. See Procedure 23-42 for more information about using the Virtual Anycast manager.

72 Click on the General tab.

73 Configure the RP IP Address parameter.

74 Click on the Anycast Peer tab.

75 Click on the Create button to create a new entry, if required. The Anycast Peer (Create) form opens.

76 Configure the Peer IP Address parameter.

77 Click on the OK button. A dialog box appears.

78 Click on the OK button. The new anycast peer entry appears on the form.

79 Click on the OK button. A dialog box appears.

80 Click on the OK button. The new anycast RP entry appears on the form.

81 Click on the following tabs to view and edit information.

- Groups
- Neighbor
- Statistics
- Faults

The Statistics and Faults tabs are unavailable for PIM in VPRN.

82 Click on the OK button. A dialog box appears.

83 Click on the Yes button. The PIM (Edit) form closes.

Procedure 23-42 To configure Anycast PIM on a router

This procedure describes how to use the Virtual Anycast Manager to configure anycast PIM on a router. The Virtual Anycast Manager automatically configures many of the supporting requirements for the protocol, which reduces operator configuration errors and assists in troubleshooting activities.



Note — The 5620 SAM does not automatically delete the supporting requirements for the protocol when you delete an anycast RP member.

You can also manually add peers to an anycast RP by navigating to the Anycast RP tab of the PIM configuration form. Ensure that PIM is enabled on the router. See Procedure 23-40 for more information.

The 5620 SAM raises an alarm when VRFs from different VPRNs are added to a single anycast RP set. You can only mismatch VRFs using methods that are not associated with the Virtual Anycast Manager; for example, by using the CLI or the PIM configuration form.

1 Choose Manage→Networking→Virtual Anycast RP from the 5620 SAM main menu. The Manage Virtual Anycast RP form opens.

2 Click on the Create button. The Virtual Anycast RP form opens with the General tab displayed.

3 Configure the parameters:

- Anycast RP Type
- Anycast RP Address
- Name
- Description
- Auto Created Interface Name

4 If the Anycast RP Type parameter value is VPRN, choose a VPRN service for the anycast RP.

i Click on the Select button. The Select Service form opens.

ii Choose a VPRN service in the list and click on the OK button. The Select Service form closes, and the service is displayed in the Service panel.

5 Click on the Apply button. The Status panel appears. The Status panel is used in step 9 of this procedure to identify configuration problems.

6 Click on the Components tab.

7 Add virtual Anycast RP members to the PIM configuration.

i Right-click on the Virtual Anycast RP Members icon and choose Add Anycast RP Member. The Enter Interface Name form opens.

ii Enter the interface name for the loopback interface. The Auto Created Interface Name parameter value appears, if configured.

iii Click on the OK button. The Enter Interface Name form closes, and the Select Local Address form opens.

iv Configure the filter criteria.

v Choose the local IP address that is used to communicate with the other RP members in the virtual anycast set and click on the OK button. The new local address entry appears on the Components tab under the Virtual Anycast RP Members icon. The new local address entry also appears under the Static RP icon.



Note — The local address is typically the system address.

The 5620 SAM automatically performs the following virtual anycast RP required configuration tasks.

- It creates a PIM-enabled loopback interface, if not present, with the RP address.
- It adds a local address to the anycast RP peer set.
- It updates the peer sets that participate in the anycast RP so that all peer sets contain the same members.
- It enables PIM on the interface that contains the local IP address.
- It creates a static RP that uses the anycast RP address. Groups must be manually created using the Components tab.

vi Repeat steps 7 i to v for each member in the virtual anycast RP.

8 Add a static group-to-RP mapping for the anycast configuration.

i Right-click on a member in the Static RP list and choose Create Static RP. The Static RP (Create) form opens.

ii Configure the parameters:

- Static Group IP Address
- Static Group Mask

iii Click on the OK button. The Static Group To RP (Create) form closes.

iv Repeat steps 8 i to iii for each static group-to-RP mapping that you want to add to the virtual anycast RP configuration. Each member needs a static RP and at least one static group-to-RP mapping. The mappings typically use the same configuration values for each member in the group.

9 Verify the status of the anycast RP for PIM configuration.

i Click on the General tab. The Status panel displays the status of the anycast RP configuration. The 5620 SAM updates the status when you add a member to or delete a member from the virtual anycast RP. You can also use the Update Status button to manually update the Status panel.

Table 23-2 lists the status check boxes that identify potential configuration problems.

Table 23-2 Anycast RP status fields

Check box	Description
Missing Group Range(s) Configurations	At least one anycast RP member does not have a group range for the anycast RP address.
Inconsistent Peer Sets	Peer sets of all the anycast RP members are not equal.
PIM not enabled on loopback interface(s)	PIM is not enabled on all loopback interfaces that are configured in the virtual anycast RP.
Only one peer configured	Only one peer is configured for anycast RP. The configuration requires two or more peers for correct functionality.
Loopback interface(s) not properly configured	At least one anycast RP member does not have a loopback interface configured with the anycast RP address.
Missing Static RP configuration(s)	A member of the virtual anycast RP does not have a static RP. Each member requires a static RP.

ii Click on the OK button. The Manage Virtual Anycast RP form reappears, and the new virtual anycast RP entry appears on the form.

iii Close the Manage Virtual Anycast RP form.

Procedure 23-43 To create a PIM interface on a base routing instance or VPRN routing instance

1 Perform one of the following:

   a Create a PIM interface on a base routing instance.

      i Choose Routing from the navigation tree view selector.

      ii Navigate to a PIM icon. The path is Routing→Router→Routing Instance→PIM.

      iii Right-click on the PIM icon and choose Create Interface. The PIM Interface (Create) form opens with the General tab displayed.

   b Create a PIM interface on a VPRN routing instance.

      i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

      ii Configure the filter criteria. A list of services appears.

      iii Choose a VPRN service.

      iv Click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

      v On the navigation tree, click on the site to which you need to add the routing instance.

      vi Expand the Routing Instance - NE System ID icon.

      vii Expand the Routing Instance icon.

      viii Expand the Protocols icon.

      ix Expand the PIM icon.

      x Right-click on the PIM instance and choose Create PIM Interface. The PIM Interface, Routing Instance (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a Layer 3 interface. The Select Interface - PIM Interface form opens.

3 Configure the filter criteria.

4 Choose an interface in the list and click on the OK button. The Select Interface - PIM Interface form closes, and the interface name appears in the Interface panel.

5 Configure the parameters:

- Description
- Administrative State
- BFD Enabled
- IPv6 BFD Enabled



Note — If you are configuring IPv6 BFD on a VPRN routing instance, you must enable the IPv6 Allowed parameter on the associated L3 access interface and set the BFD IPv6 Admin State parameter to Up on the BFD tab. See Procedure 71-38.

6 Click on the Behavior tab.

7 Click on the General sub-tab.

8 Configure the parameters:

- Hello Interval (seconds)
- Hello Multiplier
- Tracking Support
- Multicast Senders
- BSM Check Router Alert
- Improved assert
- Assert Period
- Max Groups
- Three Way Hello
- Sticky DR
- DR Priority
- Sticky DR Priority
- P2MP to LDP Tree Join Enabled

The Sticky DR Priority parameter is configurable when the Sticky DR parameter is enabled.

9 Click on the Neighbor tab, if configurable, to view and edit information. The Neighbor tab is configurable only when a neighbor PIM interface exists.

10 Click on the IPv4 or IPv6 sub-tab, as required.

11 Configure the IPv4 Administrative State or IPv6 Administrative State parameter in the States panel, as required.

12 Click on the Multicast CAC tab to add a multicast CAC policy, if required.

i Click on the Select button to choose a multicast CAC policy. The Select Multicast CAC Policy - PIM Interface form opens.

ii Choose a multicast CAC policy from the list and click on the OK button. The Multicast CAC Policy - PIM Interface form closes, and the multicast CAC policy name appears in the Multicast CAC Policy panel.

iii Configure the parameters:

- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)

iv Click on the Levels tab.

v Click on the Create button. The PIM Interface Multicast CAC level form opens.

vi Configure the parameters:

- Level ID
- Bandwidth (kbps)

vii Click on the LAG Port Down tab.

viii Click on the Create button. The PIM Interface Multicast CAC LAG Port Down form opens.

ix Configure the parameters:

- Number of Ports Down
- Level

13 Click on the OK button. The PIM Interface (Create) form closes, and an icon for the new PIM interface appears in the navigation tree below the PIM icon.

Procedure 23-44 To view an mVPN P2MP LSP object

Perform this procedure to navigate to an mVPN P2MP LSP object.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service.

4 Click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

5 On the navigation tree, click on the site on which you want to view the mVPN P2MP LSP object.

6 Expand the Routing Instance - NE System ID icon.

7 Expand the Routing Instance icon.

8 Expand the Protocols icon.

9 Click on the PIM icon. The PIM Site (Edit) form opens with the General tab displayed.

10 Click on the MVPN Inclusive Tunnel tab.

11 Click on the RSVP tab.

12 Choose an interface from the Inclusive Provider Tunnel PMSIs panel and click on the Properties button. The Inclusive RSVP PMSI Interface (Edit) form opens with the General tab displayed.

13 Click on the Properties button next to the P2MP LSP ID parameter. The P2MP LSP (View) form opens with the General tab displayed.

14 Click on the tabs to view information about the P2MP LSP object.

15 Close the P2MP LSP (View) form.

16 Close the VPRN Service (Edit) form.

17 Close the Manage Services form.

23.24 IGMP configuration procedures

The 5620 SAM supports IGMP configuration for core router functionality and IP services.

The following procedures describe how to configure IGMP.

Procedure 23-45 To enable IGMP on a router

1 Choose Routing from the navigation tree view selector.

2 Navigate to the routing instance icon. The path is Routing→Router→Routing Instance.

3 Right-click on the routing instance icon and choose Properties. The Routing Instance (Edit) configuration form opens.

4 Enable IGMP.

- i Click on the Multicast tab.
- ii Select the IGMP Enabled parameter.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Routing Instance (Edit) form closes, and an IGMP icon appears in the navigation tree below the routing instance icon.

Procedure 23-46 To configure an IGMP site on a router

Before you can configure an IGMP site on a router, you must enable IGMP on the routing instance. See Procedure 23-45 for more information.

1 Choose Routing from the navigation tree view selector.

2 Navigate to the IGMP icon. The path is Routing→Router→Routing Instance→IGMP.

3 Right-click on the IGMP icon and choose Properties. The IGMP Site (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- Administrative State
- Query Interval (seconds)
- Last Member Query Interval (seconds)
- Query Response Interval (seconds)
- Robust Count
- Group Interface Query Source IP

5 Click on the SSM Translation tab to configure SSM, if required.

i Click on the Create button to create a new entry. The SSM Translation (Create) form opens.

ii Configure the parameters:

- Start Mcast Address
- End Mcast Address
- Configured Source

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The new SSM entry appears on the form.

6 Click on the Interfaces tab to add an interface, if required.

i Click on the Create button.

ii Perform steps 4 to 14 of Procedure 23-48.

iii Click on the OK button. The new interface entry appears on the form.

7 Click on the Group Interfaces tab to view IES group interfaces added to IGMP, if required.

8 Click on the LDP Tunnel Interfaces tab to create an LDP tunnel interface entry, if required.

i Click on the Create button. The LDP IGMP Tunnel Interface (Create) form opens with the General tab displayed.

ii Click on the Select button beside the P2MP ID parameter. The Select - LDP IGMP Tunnel Interface form opens.

iii Choose an LDP tunnel interface and click on the OK button. The LDP IGMP Tunnel Interface form reappears with the information displayed.

iv Click on the Static Group/Source tab to create a static multicast entry, if required.

v Click on the Create button. The StaticGrpSrc (Create) form opens.

vi Configure the parameters:

- Static Multicast Group
- Static Source

vii Click on the OK button. A dialog box appears.

viii Click on the OK button. The new static multicast entry appears on the LDP IGMP Tunnel Interface (Create) form.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The LDP IGMP Tunnel Interface (Create) form closes.

9 Click on the RSVP Tunnel Interfaces tab to create an RSVP tunnel interface entry, if required.

i Click on the Create button. The RSVP IGMP Tunnel Interface (Create) form opens with the General tab displayed.

ii Click on the Select button beside the Lsp Name parameter. The Select - RSVP IGMP Tunnel Interface form opens.

iii Choose an RSVP IGMP tunnel interface and click on the OK button. The Select - RSVP IGMP Tunnel Interface form closes and the RSVP IGMP Tunnel Interface (Create) form reappears with the information displayed.

iv Click on the Static Group/Source tab to create a static multicast entry, if required.

v Click on the Create button. The StaticGrpSrc (Create) form opens.

vi Configure the parameters:

- Static Multicast Group
- Static Source

vii Click on the OK button. A dialog box appears.

viii Click on the OK button. The new static multicast entry appears on the form.

ix Click on the OK button. A dialog box appears. The RSVP IGMP Tunnel Interface (Create) form closes and the new tunnel entry is displayed.

x Click on the OK button. The RSVP IGMP Tunnel Interface (Create) form closes.

10 Click on the following tabs to view and edit information.

- Multicast Group/Source
- Statistics
- Faults

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The Routing Instance (Edit) form closes.

Procedure 23-47 To configure IGMP on an OmniSwitch



Note — IGMP parameters can be configured globally or for each VLAN site. The VLAN site IGMP configuration overrides the routing instance IGMP settings. You can only configure VLAN site IGMP parameters after you create the VLAN. See Procedure 66-9 for information about configuring IGMP on an OmniSwitch VLAN site.

1 Choose Routing from the navigation tree view selector.

2 Navigate to the IGMP icon. The path is Routing→ Routing Instance→IGMP.

3 Right-click on the IGMP icon and choose Properties. The IGMP (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- Administrative State
- Querying
- Spoofing
- Proxying
- Querier Forwarding
- Zapping
- Max Group Action
- Query Interval (seconds)
- Last Member Query Interval (tenths of seconds)
- Query Response Interval (tenths of seconds)
- Robust Count
- Max Group
- Protocol Version
- Router Timeout (seconds)
- Source Timeout (seconds)
- Unsolicited Report Interval (seconds)



Note — When the Administrative State parameter is set to Up, IP multicast switching is enabled on the OmniSwitch.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Routing Instance (Edit) form closes.

Procedure 23-48 To create an IGMP interface



Note — IGMP IPv6 interfaces are supported on the 7950 XRS, on the 7750 SR in chassis mode A or B with mixed mode enabled, and on the 7750 SR in chassis mode C or D.

1 Choose Routing from the navigation tree view selector.

2 Navigate to the IGMP icon. The path is Routing→Router→Routing Instance→IGMP.

3 Right-click on the IGMP icon and choose Create Interface. The IGMP Interface (Create) form opens with the General tab displayed.

4 Click on the Select button to choose a Layer 3 interface. The Select Interface - IGMP Interface form opens.

5 Configure the filter criteria, if applicable.

6 Choose an interface in the list and click on the OK button. The Select Interface - IGMP Interface form closes, and the interface name appears in the Interface panel.

7 Configure the parameters:

- Description
- Administrative State
- Administrative Version

8 Click on the Behavior tab.

9 Configure the parameters, if applicable:

- Import Policy
- Group Count
- Maximum Number of Groups
- Maximum Number of Sources
- Maximum Number of Group Sources
- Subnet Check
- Disable Router Alert Check

10 Click on the Multicast CAC tab to add a multicast CAC policy, if required.

i Click on the Select button to choose a multicast CAC policy. The Select Multicast CAC Policy - IGMP Interface form opens.

ii Choose a multicast CAC policy from the list and click on the OK button. The Multicast CAC Policy - IGMP Interface form closes, and the multicast CAC policy name appears in the Multicast CAC Policy panel.

iii Configure the parameters:

- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)
- Constraint Admin State

11 Click on the SSM Translation tab, if required.

i Click on the Create button.

ii Configure the parameters:

- Start Mcast Address
- End Mcast Address
- Configured Source
- Start Mcast Address Type
- End Mcast Address Type
- Configured Source Type

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The new SSM translation entry appears on the form.

12 Click on the Static Group/Source tab to create a static multicast entry, if required.

   i Click on the Create button.

   ii Configure the parameters:

   - Static Multicast Group
   - Static Source

   iii Click on the OK button. A dialog box appears.

   iv Click on the OK button. The new static multicast entry appears on the form.

13 Click on the following tabs to view and edit information.

   - Multicast Group
   - Multicast Group/Source

14 Click on the OK button. A dialog box appears.

15 Click on the Yes button. The IGMP Interface (Create) form closes, and an icon for the new interface appears in the navigation tree below the IGMP icon.

Procedure 23-49 To turn up or shut down an IGMP interface

1 Choose Routing from the navigation tree view selector.

2 Navigate to the IGMP icon. The path is Routing→Router→Routing Instance→IGMP.

3 Right-click on the interface icon and choose Properties. The IGMP Site (Edit) form opens.

4 Click on the Interfaces tab.

5 Turn up or shut down the IGMP interface.

   a Click on the Turn Up button to activate the interface. A dialog box appears.

   b Click on the Shut Down button to deactivate the interface. A dialog box appears.

6 Click on the Yes button to confirm the action and close the dialog box.

7 Close the IGMP Site (Edit) form.

Procedure 23-50 To view IGMP multicast reporting statistics for an IGMP site

See the *5620 SAM Statistics Management Guide* for general information about configuring and collecting statistics.

1 Choose Manage→Networking→Routing Instances from the 5620 SAM main menu. The Manage Routing Instances form opens.

2 Choose IGMP Site (IGMP) from the Select Object Type drop-down menu.

3 Click on the Search button. A list of IGMP sites appears.

4 Choose a site from the list and click on the Properties button. The IGMP Site form opens with the General tab displayed.

5 Click on the Show IGMP Multicast Reporting Statistics button. If the Show IGMP Multicast Reporting Statistics button is not visible, click on the More Actions button and choose Show IGMP Multicast Reporting Statistics. The IGMP IGMP Stats Show IGMP Multicast Reporting Statistics form opens.

6 Configure the IP address, if required.

7 Click on the OK button. The contents of the IGMP multicast report are displayed.

8 Close the IGMP IGMP Stats Show IGMP Multicast Reporting Statistics form.

Procedure 23-51 To view IGMP source statistics

See the *5620 SAM Statistics Management Guide* for general information about configuring and collecting statistics.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Click on the Search button to display a list of services.

3 Choose a service from the list and click on the Properties button. The Service (Edit) form opens with the General tab displayed.

4 Click on the Sites tab to display a list of sites.

5 Choose a site from the list and click on the Properties button. The Site (Edit) form opens with the General tab displayed.

6 Click on the Multicast tab.

7 Click on the Group Interfaces tab to display a list of group interfaces.

8 Choose a group interface from the list and click on the Properties button. The IGMP Group Interface (Edit) form opens with the General tab displayed.

9 Click on the Group Interface SAP tab.

10 Choose a group interface SAP from the list and click on the Properties button. The Group Interface SAP (Edit) form opens with the General tab displayed.

11 Click on the Group tab.

12 Click on the Search button to display a list of groups.

13 Choose a group from the list and click on the Properties button. The Group Interface SAP Group (View) form opens with the General tab displayed.

14 Click on the Source tab.

15 Click on the Search button to display a list of sources.

16 Close the Group Interface SAP Group (View) form.

17 Click on the Statistics tab.

18 Click on the Collect button to collect additional statistics.

19 Choose a statistics record from the list and click on the Properties button. The Statistics Record - Group Interface SAP Stats form opens.

20 Review the statistics and close the Statistics Record - Group Interface SAP Stats form.

21 Close the IGMP Group Interface SAP (Edit) form.

22 Close the IGMP Group Interface (Edit) form.

23 Close the Site (Edit) form.

24 Close the Service (Edit) form.

25 Close the Manage Services form.

23.25 MSDP configuration procedures

The MSDP command hierarchy consists of three levels:

- global level
- peer level and group level
- group peer level

MSDP parameters are initially applied at the global level. The parameters are inherited by the group and peer levels. Parameters can be modified and overridden on a level-specific basis.

The following procedures describe how to configure MSDP.

Procedure 23-52 To enable MSDP on a router

1 Choose Routing from the navigation tree view selector.

2 Navigate to the routing instance icon. The path is Routing→Router→Routing Instance.

3 Right-click on the routing instance icon and choose Properties. The Routing Instance (Edit) form opens.

4 Enable MSDP by performing the following steps.

i Click on the Multicast tab.

ii Select the MSDP Enabled parameter.

5 Click on the OK button. A dialog box appears.

6 Confirm the action. The Routing Instance (Edit) form closes, and an MSDP icon appears in the navigation tree below the routing instance icon.

Procedure 23-53 To configure global-level MSDP

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the MSDP icon. The path is Routing→Router→Routing Instance→MSDP.

3 Right-click on the MSDP icon and choose Properties. The MSDP (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- SA Limit
- Data Encapsulation
- Local IP Address
- RPF Lookup Sequence
- SA Cache Lifetime (seconds)
- Receive Message Rate
- Receive Message Interval (seconds)
- Receive Message Threshold
- Administrative State

5 Click on the Group tab to add a group, if required. See Procedure 23-54 for more information about how to configure a group-level MSDP.

6 Click on the Peer tab to add a peer, if required. See Procedure 23-56 for more information about how to configure a peer-level MSDP.

7 Click on the Source tab to add a source, if required. See Procedure 23-55 for more information about how to configure an MSDP source.

8 Click on the Import Policies tab.

9 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the import route policy to determine which routes are accepted from peers. The policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 22. There is no validation performed by the router to ensure the policies match.

10 Click on the Export Policies tab.

11 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the export route policy to determine which routes are advertised to peers. The policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 22. A router performs no validation to ensure the policies match.

12 Click on the following tabs to view information.

- Data Source Active
- Data Source Active Rejected
- Statistics
- Faults

13 Click on the OK button. A dialog box appears.

14 Confirm the action. The MSDP (Edit) form closes.

Procedure 23-54 To configure group-level MSDP

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the routing instance icon. The path is Routing→Router→Routing Instance→MSDP.

3 Right-click on the MSDP icon and choose Create Group. The MSDP Peer Group (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Name
- Mode
- SA Limit
- Local IP Address
- Receive Message Rate
- Receive Message Interval (seconds)
- Receive Message Threshold
- Administrative State

5 Click on the Peer tab to add a peer, if required.

6 Click on the Create button. The MSDP Peer Group (Create) form opens.

7 Configure the parameters:

- Peer Address
- SA Limit
- Local IP Address
- Default Peer
- Receive Message Rate
- Receive Message Interval (seconds)
- Receive Message Threshold
- Administrative State

8 Configure the import and export policies for the MSDP peer by performing the following steps.

i Click on the Import Policies tab.

ii Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the import route policy to determine which routes are accepted from peers. The policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 22. There is no validation performed by the router to ensure the policies match.

iii Click on the Export Policies tab.

iv Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the export route policy to determine which routes are advertised to peers. The policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 22. There is no validation performed by the router to ensure the policies match.

9 Click on the Authentication tab.

10 Configure the parameters:

- Type
- Key

11 Click on the OK button. The MSDP Peer Group (Create) form closes and a dialog box appears.

12 Confirm the action. The peer is listed on the MSDP Peer Group (Create) form.

13 Configure the import and export policies for the MSDP group by performing the following steps.

i Click on the Import Policies tab.

ii Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the import route policy to determine which routes are accepted from peers. The policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 22. There is no validation performed by the router to ensure the policies match.

iii Click on the Export Policies tab.

iv Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the export route policy to determine which routes are advertised to peers. The policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 22. There is no validation performed by the router to ensure the policies match.

14 Click on the OK button. The MSDP Peer Group (Create) form closes, and an MSDP Peer Group icon appears in the navigation tree below the MSDP Routing Instance icon.

Procedure 23-55 To configure an MSDP source

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the MSDP icon. The path is Routing→Router→Routing Instance→MSDP.

3 Right-click on the MSDP icon and choose Properties. The MSDP (Edit) form opens with the General tab displayed.

4 Click on the Source tab.

5 Click on the Create button. The MSDP Source (Create) form opens.

6 Configure the parameters:

- IP Prefix
- Mask
- SA Limit

7 Click on the OK button. The MSDP Source (Create) form closes and a dialog box appears.

8 Confirm the action. The source is listed on the MSDP (Edit) form.

9 Click on the OK button. A dialog box appears.

10 Confirm the action. The MSDP (Edit) form closes.

Procedure 23-56 To configure peer-level MSDP

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the MSDP icon. The path is Routing→Router→Routing Instance→MSDP.

3 Right-click on the MSDP icon and choose Create Peer. The MSDP Peer (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Peer Address
- SA Limit
- Local IP Address
- Default Peer
- Receive Message Rate
- Receive Message Interval (seconds)
- Receive Message Threshold
- Administrative State

5 Configure the import and export policies by performing the following steps.

i Click on the Import Policies tab.

ii Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the import route policy to determine which routes are accepted from peers. The policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 22. There is no validation performed by the router to ensure the policies match.

iii Click on the Export Policies tab.

iv Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the export route policy to determine which routes are advertised to peers. The policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 22. There is no validation performed by the router to ensure the policies match.

6 Click on the Authentication tab.

7 Configure the parameters.

- Type
- Key

8 Click on the OK button. The MSDP Peer (Create) form closes, and an MSDP Peer icon appears in the navigation tree below the MSDP Routing instance icon.

Procedure 23-57 To configure group-peer-level MSDP



Note — The parameters that you configure for a MSDP peer take precedence over the parameters that are configured for the MSDP peer group.

1 From the 5620 SAM, choose Routing from the navigation tree view selector.

2 Navigate to a peer group. The path is Routing→Router→Routing Instance→MSDP→MSDP Peer Group.

3 Right-click on the peer group icon and choose Create Peer. The MSDP Group Peer, MSDP Peer Group (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Peer Address
- SA Limit
- Local IP Address
- Default Peer
- Receive Message Rate
- Receive Message Interval (seconds)
- Receive Message Threshold
- Administrative State

5 Configure the import and export policies by performing the following steps.

i Click on the Import Policies tab.

ii Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the import route policy to determine which routes are accepted from peers. The policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 22. There is no validation performed by the router to ensure the policies match.

iii Click on the Export Policies tab.

iv Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the export route policy to determine which routes are advertised to peers. The policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 22. There is no validation performed by the router to ensure the policies match.

6 Click on the Authentication tab.

7 Configure the parameters:

- Type
- Key

8 Click on the OK button. The MSDP Group Peer, MSDP Peer Group (Create) form closes, and an MSDP Group Peer icon appears in the Navigation Tree below the MSDP Peer Group icon.

Procedure 23-58 To enable or disable MSDP peering

1 From the 5620 SAM, choose Routing from the navigation tree view selector.

2 Perform one of the following:

a Enable or disable MSDP peering in a peer group.

i Navigate to an MSDP peer group. The path is Routing→Router→Routing Instance→MSDP→MSDP Peer Group.

ii Right-click on an MSDP Peer Group icon.

b Enable or disable MSDP peering in a group peer.

i Navigate to an MSDP peer group. The path is Routing→Router→Routing Instance→MSDP→MSDP Peer Group→MSDP Group Peer.

ii Right-click on an MSDP Group Peer icon.

3 Choose one of the following menu items:

a Turn Up to activate

b Shut Down to deactivate

A dialog box appears.

4 Click on the Yes button. The state information beside the appropriate MSDP icon changes accordingly.

23.26 MLD configuration procedures

MLD is supported on the 7950 XRS, on a chassis mode C or D, and on the 7750 SR in chassis mode A or B with mixed mode enabled.

The following procedures describe how to configure MLD.

Procedure 23-59 To enable MLD on a routing instance

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Choose Network→Router→Routing Instance.

3 Right-click on the Routing Instance and choose Properties. The Routing Instance (Edit) form opens with the General tab displayed.

4 Click on the Multicast tab and enable the MLD Enabled check box.

5 Click on the OK button. The Routing Instance (Edit) form closes, and an MLD icon appears in the navigation tree below the routing instance.

Procedure 23-60 To configure MLD on a routing instance or VPRN routing instance

Perform this procedure to configure MLD on a base routing instance or on a VPRN routing instance.



Note 1 — You must first enable MLD on the base routing instance of the VPRN site. See Procedure 23-59.

Note 2 — You must ensure that the VPRN routing instance has an associated L3 access interface, and that the IPv6 Allowed parameter on the interface is enabled. You must add an IPv6 address to the L3 access interface. See Procedures 71-22 and 71-34.

1 Perform one of the following:

- **a** Configure MLD on a base routing instance.
  - **i** From the 5620 SAM GUI, choose Routing from the navigation tree view selector.
  - **ii** Choose Network→Router→Routing Instance→MLD.
  - **iii** Right-click on the MLD icon and choose Properties. The MLD, Routing Instance (Edit) form opens with the General tab displayed.
- **b** Configure MLD on a VPRN routing instance.
  - **i** Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.
  - **ii** Configure the filter criteria. A list of services appears.
  - **iii** Choose a VPRN service.
  - **iv** Click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.
  - **v** On the navigation tree, click on the site to which you need to configure MLD.

vi Expand the Routing Instance - NE System ID icon.

vii Expand the Routing Instance icon.

viii Expand the Protocols icon.

ix Right-click on the Protocols icon and choose Create MLD Site. The MLD Site (Create) form opens with the General tab displayed.

2 Configure the parameters:

- Administrative State
- Query Interval (seconds)
- Last Member Query Interval (seconds)
- Query Response Interval (seconds)
- Robust Count

3 Click on the Apply button to save the changes.

4 Click on the SSM Translation tab, and click on the Create button. The SSM Translation, Routing Instance (Create) form opens.

5 Configure the parameters:

- Start Multicast Address
- End Multicast Address
- Configured Source

6 Click on the OK button. The SSM Translation, Routing Instance (Create) form closes.

7 Click on the OK button. The MLD, Routing Instance (Edit) form closes.

Procedure 23-61 To create an MLD interface on a base routing instance or VPRN routing instance

1 Perform one of the following:

a Create an MLD interface on a base routing instance.

i From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

ii Choose Network→Router→Routing Instance→MLD.

iii Right-click on the MLD icon and choose Create Interface. The MLD Interface, Routing Instance (Create) form opens with the General tab displayed.

b Create an MLD interface on a VPRN routing instance.

i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

ii Configure the filter criteria. A list of services appears.

iii Choose a VPRN service.

iv Click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

v On the navigation tree, click on the site to which you need to add the routing instance.

vi Expand the Routing Instance - NE System ID icon.

vii Expand the Routing Instance icon.

viii Expand the Protocols icon.

ix Expand the MLD icon.

x Right-click on the MLD instance and choose Create MLD Interface. The MLD Interface, Routing Instance (Create) form opens with the General tab displayed.

2 Configure the Description parameter.

3 Click on the Select button in the Interface panel. The Select Interface - MLD Interface - Routing Instance form opens.

4 Choose a network interface that has IPv6 enabled and click on the OK button. The Select Interface - MLD Interface - Routing Instance form closes.

5 Configure the parameters in the States panel:

- Administrative State
- MLD Version

6 Click on the Behavior tab and configure the parameters:

- Disable Router Alert Check
- Maximum Number of Groups
- Query Interval (seconds)
- Maximum Response Time between Group Messages (seconds)
- Maximum Response Time For MLDv2 (seconds)

7 Click on the Import Policy tab.

8 Click on the Select button to choose an import policy.

9 Click on the Static/Group Source tab and click on the Create button. The MLD Interface Group Source Static (Create) form opens.

10 Configure the parameters:

- Group Address
- Group Source Address

11 Click on the OK button.The MLD Interface Group Source Static (Create) form closes.

12 Click on the SSM Translation tab and click on the Create button. The MLD Interface Source Specific Multicast (Create) form opens.

13 Configure the parameters:

- Start Multicast Address
- End Multicast Address
- Group Source Address

14 Click on the OK button. The MLD Interface, Routing Instance (Create) form closes.

Procedure 23-62 To configure an MLD interface on an IES L3 access interface

Perform this procedure to create an MLD interface on an IES L3 access interface. You must ensure that MLD is enabled on the site NE. See Procedure 23-59.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES service and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The IES L3 Access Interface (Edit) form opens with the General tab displayed.

7 Ensure that the IPv6 Allowed parameter is enabled.

8 Click on the Addresses tab and perform the following.

i Click on the Create button. The IP Address (Create) form opens.

ii Configure the Address ID parameter with a value greater than 1.

iii Enter an IPv6 address for the IP Address parameter.

iv Configure the Prefix Length parameter.

v Configure the parameters in the IPv6 panel:

- EUI-64
- IP Address Preferred

vi Click on the OK button. A dialog box appears.

vii Click on the OK button.

9 Click on the Multicast tab and perform the following.

i Click on the Add button. The Create Interface form opens.

ii Choose MLD from the drop-down menu and click on the OK button. The Create Interface form closes and the MLD Interface (Create) form opens with the General tab displayed.

iii Configure the Description parameter.

iv Click on the Select button in the Interface panel. The Select Interface - MLD Interface - Routing Instance form opens.

v Choose a network interface that has IPv6 enabled and click on the OK button. The Select Interface - MLD Interface - Routing Instance form closes.

vi Configure the parameters in the States panel:

- Administrative State
- MLD Version

10 Click on the Behavior tab and configure the parameters:

- Disable Router Alert Check
- Maximum Number of Groups
- Query Interval (seconds)
- Maximum Response Time between Group Messages (seconds)
- Maximum Response Time For MLDv2 (seconds)

11 Click on the Import Policy tab and perform the following.

12 Click on the Select button to choose an import policy.

13 Click on the Static/Group Source tab and perform the following.

i Click on the Create button. The MLD Interface Group Source Static (Create) form opens.

ii Configure the parameters:

- Group Address
- Group Source Address

iii Click on the OK button.The MLD Interface Group Source Static (Create) form closes.

14 Click on the SSM Translation tab and click on the Create button. The MLD Interface Source Specific Multicast (Create) form opens.

15 Configure the parameters:

- Start Multicast Address
- End Multicast Address
- Group Source Address

16 Click on the OK button. The MLD Interface Source Specific Multicast (Create) form closes.

17 Close the IES L3 Access Interface (Edit) form.

18 Close the IES Service (Edit) form.

19 Close the Manage Services form.

23.27 Bridging configuration procedures

The following procedures describe how to configure bridging.

Procedure 23-63 To configure bridging on an OmniSwitch



Caution — Changing bridge parameter values may affect the spanning tree calculations and trigger a topology change in the network.

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Locate and expand an object that represents an OmniSwitch. A Bridge Instance object appears below the OmniSwitch object.

3 Right-click on the Bridge Instance object and choose Properties. The Bridge (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- STP Mode
- Path Cost

Configure the Auto VLAN Containment parameter if you the chose the flat STP mode.

5 Configure LPS, if required.

i Click on the Learned Port Security tab. The Learned Port Security General tab is displayed.

ii Configure the parameters:

- Learning Time Window (minutes)
- Status
- Learning Time Window No Aging
- Learning Time Window Bootup Status



Note 1 — The Status parameter does not appear on the form and the Restart Timer option is dimmed until you enter a non-zero value for the Learning Time Window (minutes) parameter.

Note 2 — The Learning Time Window Expiry Status parameter is read-only and appears for OS 6400, OS 6850, OS 6850E, OS 6855, OS 9700E, and OS 9800E NEs.

Note 3 — The Learning Time Window Time Remaining (seconds) parameter is read-only and appears for OS 6900 and OS 10K NEs.

Note 4 — Click on the Restart Timer button to restart the MAC source learning timer if you need to restart dynamic MAC address learning on a port. If the Restart Timer button is not visible, click on the More Actions button and choose Restart Timer.

iii Click on the Ports tab.

iv Click on the Create button to select ports on which you want to enable learned port security. The Select Port - Bridge form opens.

v Choose one or more ports and click on the OK button. The Select Port - Bridge form closes and the selected ports appear in the Ports form.

vi Click on the Apply button to enable learned port security on the selected ports. A dialog box appears.

vii Click on the Yes button.

viii If you need to apply the same LPS properties to multiple ports but do not need to configure static MAC addresses on the ports, go to step 5xxiv.

Note — Static MAC addresses can only be added to LPS-enabled ports individually.

ix Choose a port and click on the Properties button. The Learned Port Security (Edit) form opens.

x Click on the Properties button. The Physical Port (Edit) form opens on the General tab.

xi Click on the LPS Learned MAC Entries tab.

xii Click on the Create button to add static MAC entries. The MAC Entries (Create) form opens.

Note — A port must be LPS-enabled and belong to a VLAN before you can add static MAC addresses.

xiii Click on the Select button. The Select VLAN Site - MAC Entries form opens.

xiv Configure the filter criteria. A list of VLANs appears at the bottom of the Select VLAN Site - MAC Entries form.

xv Choose a VLAN from the list.

xvi Click on the OK button. The Select VLAN Site - MAC Entries form closes.

xvii Configure the MAC Address parameter.

xviii Click on the Apply button to save the configuration.

xix Repeat steps 5xvii to 5xviii if you need to add another static MAC address to the port.

xx Click on the OK button. A dialog box appears.

xxi Click on the Yes button to close the dialog box.

xxii Click on the OK button to close the Physical Port (Edit) form. A dialog box appears.

xxiii Click on the Yes button. Go to step 5xxv.

xxiv Choose multiple ports and click on the Properties button. The Learned Port Security (Edit) form opens.

xxv Configure the parameters:

- Violation
- Administrative State
- Low MAC Range
- High MAC Range
- Max. MAC Addresses to Learn
- Max. Filtered MACs to Learn
- Trap Threshold

xxvi Click on the OK button to save the configuration and close the Learned Port Security (Edit) form.

xxvii If you need to stop the aging out of dynamic MAC addresses on the LPS port, convert the dynamic MAC addresses to static MAC addresses. Choose the port and click on the Convert to Static button. If the Convert to Static button is not visible, click on the More Actions button and choose Convert to Static.



Note — If traffic containing MAC addresses outside of the allowable MAC address range attempts to access an LPS port, the switch either restricts access to the port for that traffic or shuts the port down to all traffic. When this happens, the port is in an operationally violated state and an alarm is raised.

See Procedure 23-64 for information about how to release a violated LPS port.

6 Perform one of the following actions:

a Configure the STP Flat Mode.

b Configure the STP 1x1 Mode; go to step 25.

7 Click on the Spanning Tree tab. The STP Flat Mode CIST General tab is displayed.

8 Configure the parameters:



Caution — Changing the Protocol parameter to MSTP resets the flat bridge priority and path.

- Protocol
- Forwarding Delay (seconds)
- Max Age (seconds)
- Instance BPDU Switching
- Priority
- Hello Time (seconds)
- TX Hold Count

9 Click on the Port tab.

10 Choose one or more ports from the list.

11 Click on the Properties button. The CIST Instance Ports (Edit) form opens.

12 Configure the parameters:

- Priority
- Mode
- Admin Edge
- Restricted Role
- Path Cost
- Connection Type
- Auto Edge
- Restricted TCN

13 Click on the OK button. The CIST Instance Ports (Edit) form closes.

14 Click on the MSTI tab if you need to configure MSTI, otherwise go to step 34.



Note — In order to configure MSTI, the Protocol parameter must be set to MSTP.

15 Click on the Create button. The MST Instance (Create) form opens.

16 Configure the parameters:

- Instance Index
- Priority
- Instance Name
- Auto VLAN Containment

17 Click on the VLAN tab.

18 Click on the Create button to assign a VLAN to the MSTI. The Select VLAN Sites - MST Instance form opens.

19 Choose one or more VLANs from the list and click on the OK button. The VLANs appear on the MST Instance VLAN form.

20 Click on the OK button. A dialog box appears.

21 Click on the Yes button.

22 Click on the MST Region tab.

23 Configure the parameters:

- Region Name
- Region Revision
- Bridge Max Hops

24 Go to step 34.

25 Click on the Spanning Tree tab.



Caution — Changing the STP 1x1 Mode configuration may affect the STP calculations for this instance of the VLAN and trigger a topology change in the network.

26 Click on the STP 1x1 Mode tab.

27 Choose a 1x1 instance from the list and click on the Properties button. The VLAN STP Instance (Edit) form opens with the General tab displayed.

28 Configure the parameters:

- Protocol
- Forwarding Delay (seconds)
- Max Age (seconds)
- Instance BPDU Switching
- Priority
- Hello Time (seconds)
- TX Hold Count

29 Click on the Port tab.

30 Choose one or more ports from the list of ports that have been assigned to VLANs and click on the Properties button. The VLAN STP Instance Ports (Edit) form opens.

31 Configure the parameters:

- Priority
- Mode
- Auto Edge
- Restricted Role
- Path Cost
- Connection Type
- Auto Edge
- Restricted TCN

32 Click on the OK button. The VLAN STP Instance Ports (Edit) form closes.

33 Click on the OK button. The VLAN STP Instance form closes.

34 Click on the TLS tab.

35 Configure the TLS Mode parameter.

36 Click on the QoS tab.

37 Configure the parameters:

- QoS Status
- Trust Ports
- Default Servicing Mode
- Default Bridged Disposition
- Default Routed Disposition
- Default IGMP Disposition



Note — The Default Servicing Mode, Default Bridged Disposition, Default Routed Disposition, and Default IGMP Disposition parameters do not apply to the OS 6900 and OS 10K.

38 Click on the Apply button. A dialog box appears.

39 Click on the Yes button. The applied values for the Default Bridged Disposition, Default Routed Disposition, and Default IGMP Disposition parameters should be the same as the configured values.

40 Click on the IGMP Port Group Limit tab.

41 Configure the filter criteria. A list of ports appears.



Note — Only ports that are active (administratively Up) appear in the list.

42 Choose one or more ports from the list and click on the Properties button.

43 The IGMP Port Group Limit (Edit) or IGMP Port Group Limit - (Multiple Instances) (Edit) form opens.

44 Configure the parameters:

- Port Max Group
- Port Action

45 Click on the OK button.



Note — Click on the Multicast VLAN Port tab in the multicast VLAN IGMP site properties to view the Port Max Group and Port Action parameter information for a multicast VLAN port. You can also view the number of IGMP groups dynamically learned by the port. See Procedure 66-13 for more information.

46 If you need to configure the IGMP port group limit parameters for an inactive (administratively Down) port, click on the Create button. Otherwise, go to step 57.

47 The Select Port form opens.

48 Configure the filter criteria. A list of ports appears.

49 Choose one or more ports from the list and click on the OK button. The Select Port form closes and the selected ports appear in the list of ports.

50 Choose an inactive port from the list and click on the Properties button.

51 Configure the parameters:

- Port Max Group
- Port Action

52 Repeat steps 50 and 51 for each inactive port that you need to configure.

53 Click on the Apply button. A dialog box appears.

54 Click on the Yes button to save your configuration.



Note 1 — The inactive ports do not appear in the list of ports. Only active ports are displayed in the list. You can view the configuration of the inactive ports using the OmniSwitch CLI.

Note 2 — Click on the Multicast VLAN Port tab in the multicast VLAN IGMP site properties to view the Port Max Group and Port Action parameter information for a multicast VLAN port. You can also view the number of IGMP groups dynamically learned by the port. See Procedure 66-13 for more information.

55 Click on the MVRP tab to configure MVRP (if required).

56 Configure the parameters:

- VLAN Registration Protocol Type
- Status
- Transparent Switching Status
- Max VLAN

57 Click on the OK button. A dialog box appears.

58 Click on the Yes button. The Bridge (Edit) form closes.

Procedure 23-64 To release a violated OmniSwitch LPS port

Perform the following procedure to release a violated LPS port.

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Locate and expand an object that represents an OmniSwitch. A Bridge Instance object appears below the OmniSwitch object.

3 Right-click on the Bridge Instance object and choose Properties. The Bridge (Edit) form opens with the General tab displayed.

4 Click on the Learned Port Security tab. The Learned Port Security General tab is displayed.

5 Click on the Port tab.

6 Select one or more violated LPS ports. Violated LPS ports are highlighted in orange. When you select one or more violated ports the Release Violated Port option is enabled.

7 Click on the Release Violated Port button to release the selected ports. If the Release Violated Port button is not visible, click on the More Actions button and choose Release Violated Port. Releasing a violated port restores the port to the same operational state it was in before the violation. When a violated port is released, all MAC addresses known to the port are flushed from the switch MAC address table.

8 Close the Bridge (Edit) form.

23.28 WPP configuration procedure

The following procedure describes how to configure WPP.

Procedure 23-65 To create a web portal

1 Enable WPP on a routing instance as described in Procedure 22-1.

2 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

3 Navigate to the WPP instance icon. The path is Routing→Router→Routing Instance→WPP.

4 Right-click on the WPP icon and choose Create Web Portal. The Web Portal - Routing Instance (Create) form appears with the General tab displayed.

5 Configure the parameters:

- Name
- IP Address
- Administrative State

6 Click on the OK button. A dialog box appears.

7 Click on the OK button. The Web Portal - Routing Instance (Create) form closes.

24 — NAT

24.1 NAT overview *24-2*

24.2 Workflow to configure NAT *24-6*

24.3 NAT configuration procedures *24-6*

24.1 NAT overview

Network Address Translation, or NAT, rewrites address information in IP packets that travel between private and public networks. NAT effectively extends the public IPv4 address space; multiple end users can share one IP address. NAT provides security by preventing an internal IP address, such as an end-user address, from entering a public network.

NAT translates internal, or private, host IP address and TCP port values to external, or public, values. When NAT receives a packet from an internal host, it replaces the source address information in the packet with public address information, and forwards the packet to the destination. NAT assigns private IP addresses and ports dynamically using values from an allocated pool, but can also use values that are statically assigned to internal hosts, depending on the type of NAT deployment.

The 5620 SAM NAT support includes:

- policy-based management
- subscriber-specific implementation
- configurable port usage limits per subscriber, address range, or policy
- reserved port ranges for specified forwarding classes that are exempt from port usage limits
- configurable protocol timeout periods for efficient resource management

The NAT configuration on a routing instance includes:

- one or more NAT address pools that are associated with local ISA-NAT groups
- a NAT policy that specifies port ranges and operational parameters
- host address match criteria
- one or more NAT destinations

A 5620 SAM operator assigns port ranges in an address pool configuration. Port ranges specify the number of ports that are allocated to a subscriber for mapping to host sessions. If all ports for a subscriber are in use, additional port assignments cannot occur and host sessions are rejected. This function helps to prevent the flooding of NAT by a virus attack or multiple peer-to-peer file transfers. You can override a port range limit by configuring a range of reserved ports that are assigned based on the traffic forwarding class.



Note — You cannot use ports 0 to 1023, which are called the well-known ports or privileged ports, in a NAT configuration.

To provide equitable and timely NAT resource allocation to hosts, you can specify timeout values in a NAT policy for protocols such as ICMP, TCP, and UDP. NAT ends a host session after the timeout period, for example, when a TCP handshake takes an excessive amount of time.

The NAT drain function is a mechanism that is used to gracefully remove the host sessions associated with an address range in a NAT address pool. When an address range is in the draining state, NAT drops new session requests for the address range. After an existing session associated with a draining address range closes, a new session for the same host is created using a different address range. The drain

function removes an address range only when there are no sessions associated with the address range. See Procedure 24-10 for information about using the NAT drain function.

You can view general NAT statistics, for example, address pool allocation and session counts for different protocols on the Statistics tab of an ISA-NAT group member properties form.



Note — The 5620 SAM does not record detailed NAT session information such as session duration or packet counts. You can obtain this information from a request to a participating NE.

The 5620 SAM supports the following NAT deployment types:

- L2-aware—Hosts of the same subscriber can share a private address, and are assigned public addresses from a pool in a base routing instance.
- large-scale—Each host can have a unique static or dynamic private address, and is assigned a public address from a pool in a VPRN routing instance.

L2-aware NAT

In L2-aware NAT, a NAT policy is associated with a subscriber profile that is applied to an IES SAP. The policy specifies an address pool on the base routing instance. When DHCP assigns a private IP address that is in an L2-aware NAT address range, NAT assigns a public IP address to the host packets. See chapter 70 for information about configuring NAT in an IES.



Note 1 — A NAT configuration on a base routing instance applies to each IES site on the NE.

Note 2 — A NAT policy that is specified in a subscriber profile redirects the IPv4 traffic for the subscriber to NAT.

Large-scale NAT

Large-scale NAT, or LSN, is required when each host in a customer VPRN service has a unique private IP address and requires a unique public IP address, for example, in mobile network deployments. Large-scale NAT is used between routing instances. A customer VPRN routing instance provides host access and forwards packets through NAT to a VPRN or through an IES to an NE routing instance, which provides public network access.

A VPRN routing instance requires an ACL IP filter or static route to transmit host traffic through the NAT function, and uses an address pool in the VPRN routing instance. You can configure large-scale NAT to statically and dynamically assign private addresses. See chapter 71 for information about configuring NAT in a VPRN service. See "Static port forwarding" in this section for more information about configuring NAT to use static private addresses.

You can use the 5620 SAM Statistics Plotter to plot real-time LSN subscriber host statistics on a base or VPRN routing instance. See Procedure 24-9 for information.

Static port forwarding

In a large-scale NAT deployment, you can configure NAT to assign static private addresses to subscriber hosts using static port forwarding. Static port forwarding ensures that an internal host uses the same private IP address and port each time they connect to the network. You can use the 5620 SAM to configure static port forwarding for TCP and UDP independently.

A standby routing instance can be specified to create static port forwards for pools in a redundant configuration. The 5620 SAM identifies the active pool from the two specified NEs and creates a static port forward on the active pool. In the event of a wildcard static port forward request, if there is a switch-over of the active pool, the 5620 SAM attempts to create the static port forward on the other pool. If there is a second pool switch-over, the static port forward is not created.

See chapter 71 for information about configuring static port forwarding in a VPRN service. See chapter 65 for information about configuring L2Aware static port forwarding on a residential subscriber instance.

Dynamic block reservation

To prevent starvation of dynamic port blocks for subscribers that use static port forwarding, dynamic port blocks can be reserved for the lifetime of the static port forward. Dynamic port blocks are associated with the same inside IP addresses that are associated with the static port forward. A log entry is not generated until the dynamic port block is used.

At the time of static port forward creation:

- If the corresponding dynamic port block mapping (same inside IP address) does not exist, dynamic port block(s) are reserved and associated with the same inside IP addresses used in the static port forward. No log entries are generated for the reserved dynamic port blocks.
- If corresponding dynamic mappings (relative to the inside IP address) exist, the existing port block is reserved (or kept) after the last mapping within it has expired. The reserved dynamic port block(s) continue to be associated with the same inside IP address until the static port forward is deleted. A log entry is generated when the last mapping in the dynamic port block expires (even if the dynamic port block continues to be reserved).

NAT pools

A NAT pool is a range of public IP addresses that are translated to inside private IP addresses in a Large Scale or L2 Aware NAT configuration. A NAT pool is required in order to configure a NAT policy, as well as static port forwarding, DS Lite, and NAT 64.

NAT policies

A NAT policy defines general NAT properties and associates a NAT address pool with an ISA-NAT group on the same NE. A NAT policy is associated with a subscriber profile for L2-aware NAT in an IES or VPRN service, or for large-scale NAT in a VPRN service.

A NAT pool must be assigned to the local NAT policy before the NAT policy can be associated with the NAT configuration. A NAT policy is required in order to configure DS Lite, NAT 64, and NAT subscriber identification.

ISA-NAT groups

An ISA-NAT group provides a redundant NAT function for routing instances using ISA Broadband Applications MDAs. The group can contain up to six MDAs in a warm redundancy configuration. For an ISA-NAT group to be operational, at least one member MDA must be in the active role. See the NE documentation for more information about NAT deployment.



Note 1 — You can install an ISA-NAT Broadband Applications MDA in an IOM3-XP.

Note 2 — The same ISA Broadband Applications MDA can belong to an ISA-NAT group and an ISA-LNS group.

NAT Destinations

A NAT destination prefix applies NAT to all traffic that matches a given route. A NAT Destination cannot be configured in conjunction with a NAT policy that points to a NAT pool that resides in the same service. Such a configuration would result in a routing loop.

NAT 64

NAT 64 allows IPv6 hosts to connect to IPv4-only servers, mapping their inside IPv6 addresses to outside IPv4 addresses. NAT 64 configuration requires support for IPv6 (chassis mixed mode) on the NE. You must assign a NAT policy to the NAT configuration before enabling NAT 64. IP fragmentation can be configured to allow IPv6 packet fragmentation before transmission.

DS Lite

DS Lite is intended for network operators that have an IPv6-only access network, but IPv4-only CPEs. The inside IPv4 host information is encapsulated into a 4to6 tunnel that runs over the IPv6 network. At the other end, the IPv4 address is de-encapsulated and translated to an outside IPv4 address via CGN. You must assign a NAT policy to the NAT configuration before enabling DS Lite. IP fragmentation can be configured to allow IPv6 packet fragmentation before transmission if the packets are larger than the tunnel MTU for a given DS Lite address.

Deterministic NAT

Deterministic NAT is a mode of operation in which the inside IP address and source ports are deterministically mapped to the outside IP address and port range at the time of configuration. Each inside IP address is permanently mapped to an outside IP address and a dedicated port block. The dedicated port block is referred to as the deterministic port block. Deterministic mapping can be automatically extended by a dynamic port block in cases where a deterministic port range runs out of ports. Because a simple formula is used to determine the inside IP address based on the outside IP address and port, there is no need for NAT logging.

The NAT deterministic script generates an offline calculation of the deterministic NAT map entries. You can save the script results to a folder on a remote server by specifying a URL for the server in the local NE properties.

In the 5620 SAM, inside IP addresses are configured in the form of prefixes. Any inside prefix on any routing instance can be mapped to any deterministic pool on any routing instance, including the deterministic pool in which the inside prefix is defined. The mapping between the inside prefix and the deterministic pool is achieved through a NAT policy that is referenced for each individual prefix. IP addresses from the prefixes on the inside are distributed over the IP addresses defined in the outside pool referenced by the NAT policy.

A port block is a collection of ports that is assigned to a subscriber. A deterministic LSN subscriber can have only one deterministic port block that can be extended by multiple dynamic port blocks. All port blocks for an LSN subscriber must be allocated from a single outside IP address.

A port range is a collection of ports that can spawn multiple port blocks of the same type. For example, a deterministic port range includes all ports that are reserved for deterministic consumption. A dynamic port range is a total collection of ports that can be allocated in the form of dynamic port blocks.

24.2 Workflow to configure NAT

1. Provision an ISA-NAT group on an ISA MDA. See Procedure 24-1.
2. Configure a NAT policy. See Procedure 24-2.
3. Associate a NAT policy with a subscriber profile. See Procedure 54-18.
4. Configure NAT on a routing instance. See Procedure 24-3.

24.3 NAT configuration procedures

The following procedures describe how to configure NAT.

Procedure 24-1 To configure an ISA-NAT group

Perform this procedure to create and configure an ISA-NAT group.

1. Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.
2. Expand an NE object in the equipment navigation tree.
3. Expand the Logical Groups object in the equipment navigation tree.

4 Perform one of the following:

a To create an ISA-NAT group, right-click on the ISA-NAT Groups object and choose Create ISA-NAT Groups. The ISA-NAT Group (Create) form opens with the General tab displayed. Configure the Group Number parameter.

b To configure an ISA-NAT group, expand the ISA-NAT Groups object, right-click on the ISA-NAT group that you want to configure and choose Properties from the contextual menu. The ISA-NAT Groups (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Description
- Active MDA Limit
- Reservation Count
- Session Watermark High
- Session Watermark Low
- Current OLC State
- Revert OLC State

The Current OLC State and Revert OLC State parameters are configurable when you click on the Apply button on the ISA-NAT Group form.

6 Click on the Select button beside the RADIUS Accounting Policy parameter. The Select Policy - ISA-NAT Group form opens with a list of available NAT RADIUS accounting policies.

7 Select a NAT RADIUS accounting policy from the list and click on the OK button. The Select Policy - ISA-NAT Group form closes and the ISA-NAT Group form reappears with the RADIUS accounting policy information displayed.

8 Click on the Apply button. The ISA-NAT Group form refreshes with additional tabs.

9 Click on the ISA-NAT MDA tab.

10 Click on the Create button. The ISA-NAT Group MDA (Create) form opens.



Note — You can configure up to six ISA-NAT group members. Each group member must be an ISA Broadband Applications MDA.

11 Click on the Select button. The Select Daughter Card form opens.

12 Choose an MDA in the list and click the OK button. The Select Daughter Card form closes, and the ISA-NAT Group MDA (Create) form displays the MDA identifier in the Slot Name field.

13 Click on the OK button. The ISA-NAT Group MDA (Create) form closes and a dialog box appears.

14 Click on the OK button. The ISA-NAT Group form lists the MDA.

15 Repeat steps 10 to 14 to configure another ISA-NAT Group MDA, if required.

16 Click on the General tab.

17 Configure the Administrative State parameter.



Note — You can set the Administrative State parameter to Up only when the ISA-NAT group contains at least one MDA and when the Active MDA Limit parameter is set to a value greater than 0.

18 Click on the OK button. A dialog box appears.

19 Click on the Yes button. The ISA-NAT Group form closes.

Procedure 24-2 To configure a NAT policy

Perform this procedure to configure a NAT policy for a large-scale or L2-aware NAT implementation.

1 Choose Policies→ISA Policies→NAT from the 5620 SAM main menu. The NAT Policies form opens.

a Create a new NAT policy by clicking on the Create button. The NAT Policy (Create) form appears with the General tab displayed.

b Configure an existing NAT policy by clicking on an item in the list and clicking on the Properties button. The NAT Policy (Edit) form appears with the General tab displayed.

2 Configure the parameters:

- Displayed Name
- Description
- Filtering
- ALG Protocols
- UDP Inbound Refresh
- TCP Maximum Segment Size
- Port Reservation Count
- High Watermark (%)
- Low Watermark (%)
- Max Port Blocks
- Max Port Forwarding Entries
- Session Limit
- Reservation Count
- Session High Watermark (%)
- Session Low Watermark (%)
- Priority Session Forwarding Class Set
- TCP Established
- TCP Transitory
- TCP Syn
- TCP Time Wait
- ICMP Query
- SIP
- UDP
- UDP Initial
- UDP DNS

3 Click on the Select button in the IPFIX Export Policy panel and choose an IPFIX export policy from the Select IPFIX Export Policy form.

4 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 42 for more information.

5 Assign a NAT pool to a local definition of the policy, as required.



Note — The policy must be distributed to the NE on which the NAT pool is configured before the local definition of the policy can be configured.

i Click on the Local Definitions tab.

ii Click on the Search button. A list of NEs to which the policy has been distributed appears.

iii Click on an item in the list and click on the Properties button. The NAT Policy, Local Policy form appears.

iv Ensure that the Distribution Mode field of the local policy is set to Local Edit Only. Click on the Switch Mode button to change the distribution mode.

v Click on the Select button next to the Router Name field and choose a NAT pool from the Select NAT Pool dialog box.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The NAT Policy form closes.

8 Close the NAT Policies manager.

Procedure 24-3 To configure NAT on a routing instance

Perform this procedure to configure NAT on a base routing instance, or on a VPRN routing instance.

1 Choose Routing from the navigation tree view selector.

2 Navigate to a routing instance by choosing Network→NE→Routing Instance.

3 Right-click on the Routing Instance icon and choose Properties from the contextual menu. The Routing Instance (Edit) form opens with the General tab displayed.

4 Click on the NAT tab.

5 On the NAT Configuration sub-tab, do one of the following:

a Create a new NAT configuration by clicking on the Create button. The NAT Configuration (Create) form appears with the Outside tab displayed.

b Configure an existing NAT configuration by clicking on an item in the list and clicking on the Properties button. The NAT Configuration (Edit) form appears with the Outside tab displayed.

Click on the Hints button at the bottom of the form to display information about the various components and options available to a NAT configuration.

6 Configure the MTU parameter.

7 Use the Select button to choose an ACL filter from the Select Upstream IP Filter form, if required.

8 Configure NAT pools, as required.

i Click on the Create button to create a new NAT pool, or select an existing NAT pool in the list and click on the Properties button. The NAT Pool form appears with the General tab displayed.

ii Configure the parameters, as required:

- Displayed Name
- Description
- Subscriber Limit
- Deterministic NAT Port Reservation
- Port Forwarding Dynamic Block Reservation
- Exported Address Prefix
- Prefix Length
- Monitored Address Prefix
- Prefix Length
- NAT Pool Type
- Administrative State
- Pool Mode
- Port Reservation Type
- Port Reservation Value
- Port Forward Range End
- High Watermark (%)
- Low Watermark (%)



Note — The Deterministic NAT Port Reservation and Port Forwarding Dynamic Block Reservation parameters are mutually exclusive. If one is configured, the other is disabled. The Port Forwarding Dynamic Block Reservation parameter applies only to large scale NAT pools.

iii Click on the Select button and choose an ISA-NAT group from t Select ISA-NAT group form.

iv Click on the NAT Pool Ranges tab.

v Click on the Create button. The Pool Range form opens.

vi Configure the parameters:

- Description
- Range Start
- Range End

vii Click on the OK button. A dialog box appears.

viii Click on the OK button. The Pool Range form closes, and the NAT Pool form lists the pool range.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The NAT Pool form closes, and the NAT Configuration form lists the NAT pool.

xi Repeat steps i to x to add another pool, if required.

9 Click on the Inside tab. The General sub-tab is displayed.

i Configure Deterministic NAT parameters, if required.

- Classic LSN Maximum Subscriber Limit
- DS Lite Maximum Subscriber Limit

ii Click on the Select button and choose a NAT policy from the Select NAT policy form.



Note — The NAT policy you choose must be distributed to the local NE, and the local definition of the NAT policy must be configured with a NAT pool. See Procedure 24-2.

iii Click on the Apply button. A dialog box appears. Click on the Yes button.

iv Configure the parameters, if required.

- NAT 64 Enabled

Redundancy panel:

- Peer Address
- Steering Route Address Prefix
- Prefix Length

DS Lite panel:

- Administrative State
- Subscriber Prefix Length

NAT Subscriber Identification panel:

- Description
- Administrative State
- Drop Unidentified Traffic

v In the RADIUS Proxy Server panel, click on the Select button next to the Routing Instance field and choose a routing instance from the Select Routing Instance form.

vi Click on the Select button next to the RADIUS Proxy Server Name field and choose a RADIUS proxy server from the RADIUS Proxy Server form.

Note — The selection of the RADIUS Proxy Server Name is dependent on the selected routing instance. You can select only servers enabled for accounting.

vii In the RADIUS Vendor Information panel, click on the Select button next to the Attribute Type field and choose an attribute type from the Select RADIUS Attribute form. The attribute type information is displayed in the fields of the RADIUS Vendor Information panel.

10 Perform the following steps to add an IP address for L2-aware NAT forwarding, as required.

i Click on the L2 Aware IP Addresses sub-tab.

ii Click on the Create button. The L2 Aware IP form opens.

iii Configure the parameters:

- IP Address
- Prefix Length

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The L2 Aware IP form closes, and the NAT Configuration form lists the IP address.

vi Repeat steps ii to v to add another IP address, if required.

11 Perform the following steps to add a DS Lite address, as required.

i Click on the DS Lite Address sub-tab.

ii Click on the Create button. The Dual Stack Lite Address form opens.

iii Configure the and parameters.

- AFTR IP Address
- Tunnel MTU
- Address IP Fragmentation

Note — If address IP fragmentation is enabled, the Tunnel MTU parameter value must be equal to or greater than 1232 bytes.

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Dual Stack Lite Address from closes and the NAT Configuration form lists the DS Lite address.

12 Perform the following steps to configure NAT 64, as required.



Note — In order to configure NAT 64, you must have configured the NAT 64 Enabled parameter in step 9.

i Click on the NAT 64 sub-tab.

ii Configure the Administrative State and Subscriber Prefix Length parameters.

iii If the Administrative State parameter was set to Out Of Service in step ii, configure the following parameters:

- Nat Destination Prefix
- Nat Destination Prefix Length
- IPv6 MTU
- Drop UDP With Zero Checksum
- Ignore IPv6 TC and Set IPv4 ToS
- Ignore IPv4 ToS and Set IPv6 TC
- Insert IPv6 Fragment Header
- IP Fragmentation



Note — If IP fragmentation is enabled, the IPv6 MTU parameter value must be equal to or greater than 1280 bytes.

13 Perform the following steps to add an inside NAT destination address, as required.

i Click on the Destination Prefixes sub-tab.

ii Click on the Create button. The Destination Prefix form opens.

iii Configure the parameters:

- IP Address
- Prefix Length

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Destination Prefix form closes, and the NAT Configuration form lists the destination address.

vi Repeat steps ii to v to add another destination address, if required.

14 Perform the following steps to add an inside NAT deterministic prefix, as required.



Note — In order to configure a NAT deterministic prefix, you must have configured one of the Deterministic NAT parameters in step 9.

i Click on the Deterministic Prefixes sub-tab.

ii Click on the Create button. The Deterministic NAT Prefix form opens.

iii Configure the parameters:

- Subscriber Type
- Prefix Address
- Prefix Length
- Administrative State
- Map Creation Disabled

iv Click on the Select button next to the NAT Policy field and choose a NAT policy from the Select NAT Policy form.

v In the Deterministic Map panel, click on the Create button. The Deterministic NAT Map form opens.

vi Configure the parameters:

- Start Address
- End Address
- To Address

vii Click on the OK button. The Deterministic NAT Prefix form is updated with the new deterministic map.

viii Repeat steps v to vii to add another deterministic map, if required.

ix Click on the OK button in the Deterministic NAT Prefix form. The form closes, and the NAT Configuration form lists the deterministic prefix.

x Repeat steps ii to ix to add another deterministic prefix, if required.

15 Perform the following steps to configure NAT port forwarding, if required.

i Click on the NAT Port Forwarding tab.

ii Click on the Static sub-tab.

iii Click on the Create button. The NAT Static Port Forwarding form opens.

iv Configure the parameters:

- Type
- Inside IP Address
- Outside IP Address
- Inside Port
- Protocol
- Outside Port
- Lifetime (seconds)
- B4 Address
- AFTR Address



Note — You cannot specify the same set of Inside Port and Protocol values in more than one static port mapping to an Inside IP Address.

You can specify the same Outside Port value in multiple mappings to an Inside IP Address.

The B4 Address and AFTR Address parameters apply only to DS Lite LSN configurations.

v If a redundant pool configuration is in use, click on the Select button next to the Routing Instance field and choose the site of the standby pool from the Select Routing Instance form.

vi Click on the OK button. The NAT Static Port Forwarding form closes, and the NAT Configuration form lists the new entry.

vii Repeat steps iii to vi to assign large scale NAT static port forwards, if required.

16 Synchronize NAT static port forwards, if required.

i Click on the Static sub-tab.

ii Configure the Resync Static and Dynamic parameter, if required. If this parameter is enabled, both static and dynamic forwarders are retrieved from the NE.

Static port forwards are persisted in the 5620 SAM database. Dynamic port forwards are retrieved from the NE, and are retained in the 5620 SAM GUI only for the duration of the current session.

iii Click on the Resync NAT Port Forward button. A confirmation dialog box appears.

iv Click on the Yes button.

17 Click on the OK button. A dialog box appears.

18 Click on the Yes button. The NAT Configuration form closes, and the NAT configuration is listed on the Routing Instance form.

Procedure 24-4 To configure a NAT deterministic script on a remote server

1 Choose Equipment from the navigation tree view selector.

2 Right-click on the NE on which you want to configure a NAT deterministic script and choose Properties. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Globals tab.

4 Click on the Subscriber Management tab.

5 Configure the Remote URL parameter using the following syntax:

[{ftp://|tftp://}<*login*>:<*password*>@<*remote_address*>/]
[<*path_file*>]

where...

<*login*> is the login name of the remote server.

<*password*> is the login password of the remote server.

<*remote_address*> is the IP address of the remote server.

<*path_filename*> is the path to the folder on the remote server where the mappings are stored.

6 Click on the Apply button and then confirm the change.

7 Click on the Save Script button to save the current deterministic NAT mappings to a file on the specified remote server.

8 If required, click on the Resync button to update the read-only information in the Save Needed, Last Saved Result, and Last Saved Time fields.

If a change occurs on the local NE that affects the deterministic NAT mappings, the Save Needed parameter changes to Yes, indicating that you must click on the Save Script button to update the mappings.

9 Click on the OK button. A dialog box opens.

10 Click on the Yes button. The Network Element (Edit) form closes.

Procedure 24-5 To create an IPFIX export policy

Use this procedure to create an IPFIX export policy for use with an NAT policy.

1 Choose Policies→IPFIX Export Policy from the 5620 SAM main menu. The IPFIX Export Policy form opens.

2 Click on the Create button. The IPFIX Export Policy (Create) form appears.

3 In the General tab, configure the following parameters:

- Displayed Name
- Description

4 Click on the IPFIX Collectors tab.

5 Click on the Create button to create a new collector definition. The IpfixCollector form opens.

6 Configure the following parameters:

- Displayed Name
- Administrative State
- Router Instance Type
- IPFIX Collector Address
- IPFIX Collector Source Address
- Default
- MTU
- Refresh Timeout

7 If you specified a Router Instance Type of VPRN, perform the following:

   i Click on the Select button. The Select vprnPointer form opens.

   ii Configure the filters and click on the Search button. A list of VPRN pointers appears.

   iii Select a VPRN pointer and click on the OK button.

8 Click on the OK button. The IpfixCollector form closes.

9 Click on the Apply button. The policy is saved and is ready to be distributed.

Procedure 24-6 To view reserved IP address and reserved block information on an ISA-NAT group

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the ISA-NAT group object where you want to view reserved IP address and reserved block information. The path is Network→*NE*→Logical Groups→ISA-NAT Groups→ISA-NAT Group *n*.

3 Right-click on an ISA-NAT Group *n* icon and choose Properties. The ISA-NAT Group (Edit) form opens with the General tab displayed.

4 Click on the ISA-NAT Members tab.

5 Click on the Search button. A list of ISA-NAT members is displayed.

6 Select an ISA-NAT member from the list and click on the Properties button. The ISA-NAT Member form opens with the General tab displayed.

7 Reserved IP address and reserved block information is viewable under the following read-only parameters:

- IP Addresses Reserved
- Blocks Reserved

   Click on the Resync button to update the IP Address Reserved and Blocks Reserved values to the most recent information available on the MDA.

8 Click on the Close button. The ISA-NAT Member form closes.

9 Close the ISA-NAT Group (Edit) form.

Procedure 24-7 To view ISA-NAT object information

Use this procedure to perform an on-demand retrieval of large-scale NAT entries, based on a routing instance ID. Search results can be further constrained by specifying an inside address (for a classic LSN host, DS Lite subscriber, or NAT64 subscriber) or an outside address and start port number (for an LSN block allocation).

1 Click Manage→ISA Functions→ISA-NAT. The Manage ISA-NAT form appears.

2 Select an object type from the drop-down list:

- Classic LSN Host
- DS Lite Subscriber
- ISA-NAT Group
- LSN Block Allocation
- NAT64 Subscriber

3 Depending on the object type you selected in step 2, configure the following parameters, as required:

- Site ID
- Routing Instance
- Inside Address
- Outside Address
- Start Port #

4 Click on the Search button. A list of ISA-NAT object entries is displayed.

5 Select an entry in the list and click on the Properties button. A read-only object properties form appears.

6 Review the information and click on the Cancel button to close the form.

7 Click on the Close button. The Statistics Record form closes.

8 Close the Manage ISA-NAT form.

Procedure 24-8 To configure statistics on an ISA-NAT group

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the ISA-NAT group object where you want to configure statistics. The path is Network→*NE*→Logical Groups→ISA-NAT Groups→ISA-NAT Group *n*.

3 Right-click on the ISA-NAT Group *n* icon where you want to configure statistics and choose Properties. The ISA-NAT Group (Edit) form opens with the General tab displayed.

4 To configure ISA Member statistics, ISA Member Usage statistics, or Policy statistics, click on the ISA-NAT MDA tab.



Note — You can also collect ISA NAT Member statistics or ISA NAT Member Usage statistics (but not NAT Policy statistics) from the ISA-NAT Members tab. The procedure for collecting statistics is the same as is outlined below.

5 Click on the Search button. A list of ISA-NAT MDAs is displayed.

6 Select an ISA-NAT MDA from the list and click on the Properties button. The ISA-NAT Group MDA (Edit) form opens.

7 Click on the Statistics tab.

8 In the Select Object Type area, choose one of the following from the contextual menu:

- ISA NAT Member Stats
- ISA NAT Member Usage Stats
- NAT Policy Stats

9 Click on the Collect button.

10 A statistics record appears on the ISA-NAT Group MDA (Edit) form. Select the record.

11 Click on the Properties button. The Statistics Record form opens.

12 View the read-only statistics parameter values for the ISA-NAT group MDA.

13 Click on the Close button. The Statistics Record form closes.

14 Close the ISA-NAT Group MDA (Edit) form.

15 Close the ISA-NAT Group (Edit) form.

Procedure 24-9 To plot LSN subscriber host statistics

Perform this procedure to view LSN subscriber host statistics data in graphical form.



Note — You can plot only real-time statistics data for a subscriber host. The 5620 SAM does not retain historical subscriber host information.

1 Perform one of the following.

   a Plot the statistics data from a base routing instance. Perform the following steps.

      i Choose Routing from the navigation tree view selector.

      ii Navigate to a routing instance. The path is Network→NE→Routing Instance.

      iii Right-click on the Routing Instance icon and choose Properties from the contextual menu. The Routing Instance (Edit) form opens with the General tab displayed.

   b Plot the statistics data from a VPRN routing instance. Perform the following steps.

      i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

      ii Configure the filter criteria, as required, and click on the Search button. A list of services is displayed.

      iii Select a VPRN service in the list and click on the Properties button. The VPRN Service (Edit) form opens.

      iv Expand the Sites object in the service navigation tree.

      v Select a routing instance in the service navigation tree. The Site (Edit) form opens.

2 Click on the NAT tab.

3 Perform one of the following.

   a To plot host statistics for a DS Lite subscriber, click on the NAT DS Lite Subscribers tab.

   b To plot host statistics for a NAT 64 subscriber, click on the NAT64 Subscribers tab.

   c To plot statistics for classic LSN hosts, click on the Classic LSN Hosts tab.

4 Click on the Search button. A list of subscriber hosts is displayed.

5 Select a subscriber host in the list and click on the Properties button. The subscriber host properties form opens.

6 Click on the More Actions button and choose Plotter→New Plot. The Statistics Plotter window opens.

See "Graphing statistics" in the *5620 SAM Statistics Management Guide* for information about using the 5620 SAM Statistics Plotter.

7 View the plotted statistics data.

Save the tabular data or plot graph, as required.

8 Close the open forms.

Procedure 24-10 To start or stop a NAT address-pool drain operation

Perform this procedure to control the removal, or draining, of the host sessions associated with a NAT pool address range.

1 Choose Routing from the navigation tree view selector. The navigation tree displays the routing view.

2 Navigate to a routing instance that has one or more configured NAT pools. The path is Network→*NE*→Routing Instance.

3 Right-click on the routing instance icon and choose Properties from the contextual menu. The Routing Instance (Edit) form opens.

4 Click on the NAT Configuration tab.

5 Click on the Search button. A list of NAT configurations is displayed.

6 Choose the required NAT configuration in the list and click on the Properties button. The NAT Configuration (Edit) form opens with the General tab displayed.

7 Click on the NAT Pools tab.

8 Click on the Search button. A list of address pools is displayed.

9 Choose the required address pool in the list and click on the Properties button. The NAT Pool (Edit) form opens.



Note — You can also select multiple address pools and use the Drain or Stop Drain buttons to control the draining for the selected address pools, as described in subsequent procedure steps.

10 To start a drain operation on the address pool, click on the Drain button. The number of host sessions that are associated with the address range decreases as sessions close.

11 To stop an active drain operation on the address pool, click on the Stop Drain button. New host sessions can use the address range.

12 Close the open forms, as required.

25 — MPLS

25.1 MPLS overview *25-2*

25.2 Sample MPLS configuration *25-11*

25.3 Workflow to configure MPLS *25-12*

25.4 MPLS procedures *25-13*

25.1 MPLS overview

The 5620 SAM supports the configuration and provisioning of MPLS paths and LSPs.

MPLS is a data-carrying mechanism that emulates some properties of a circuit-switched network over a packet-switched network. MPLS prepends a packet with an MPLS header that is comprised of labels in a stack. As an NE forwards a packet through an MPLS network, it examines the top label for routing instructions and pops it off the stack; the contents below the label stack are not examined. The label stack is not removed until it reaches the egress NE.

MPLS uses one or more IGPs, such as IS-IS, OSPF, or RIP, to forward packets. Regardless of the IGP chosen, the MPLS configuration is the same. An advantage of MPLS is that if more than one IGP is enabled, it continues to work when another protocol fails. See chapter 23 for more information on IS-IS, OSPF, and RIP.

MPLS can be used as the underlying transport mechanism for service tunnels. For MPLS to be used as such, an MPLS mesh and an LSP mesh must be created before the tunnel is created. Since LSPs and service tunnels are unidirectional, they must be created in both directions. See chapter 27 for more information about service tunnels.

When MPLS is enabled on a 5620 SAM-managed NE routing instance, the 5620 SAM displays an MPLS instance below the routing instance in the network view of the navigation tree. Using this view, you can perform various functions on the MPLS instance, for example, assign an L3 interface to an MPLS instance.

If a link, NE, or path fails, MPLS can determine a redundant path by using fast reroute. Fast reroute uses an alternative NE to complete the failed LSP. Fast reroute provides the following types of route protection.

- Many-to-one—one backup route is maintained for multiple protected LSPs on an NE.
- One-to-one—a separate backup route is maintained for each protected LSP on an NE algorithm.

You can list and view MPLS objects such as MPLS and RSVP instances and interfaces, static and dynamic LSPs, cross connections, and MPLS paths using the 5620 SAM Manage MPLS Objects form.

LSPs

An LSP is a path through an MPLS network that is set up based on criteria in a forwarding equivalency class, or FEC. A FEC is a set of characteristics that define how NEs in an MPLS network forward packets that are bound to an MPLS label. A FEC includes specifications such as the destination IP address and QoS parameters. A FEC is associated with a specific LSP, but an LSP may be used for multiple FECs.

An LSP begins at a PE device called an LER, which is the ingress NE that prepends a label to a packet based on a FEC and sends the packets to the next transit NE in the path. The transit NE swaps the packet label for a new one, and sends the packet to the next NE. The LER that acts as the egress PE NE removes the label and forwards the packet according to the header of the next layer, for example, IP.

LSPs are unidirectional; they enable the label switching of a packet through an MPLS network from one endpoint to another. Bidirectional communication through an MPLS network requires the configuration of an LSP in the opposite direction.

The types of LSPs are the following.

- Static LSPs specify a static path through an MPLS network. All transit NEs require manual configuration with LSP labels and require no signaling protocol, such as LDP or RSVP.
- Bypass-only LSPs are LSPs with manually configured bypass tunnels on Point-of-Local-Repair (PLR) NEs. Such LSPs are used exclusively for the purpose of bypass protection.
- Dynamic, or signaled LSPs, use a protocol such as LDP or RSVP. The signaling protocol allows an ingress NE to dynamically assign labels to an egress NE. You must configure the ingress NE, but not the transit NEs in an LSP. LDP LSPs are not explicitly defined. The downstream unsolicited (DU) method configures them automatically through the network.
- Point-to-Multipoint LSPs allow the source of multicast traffic to forward packets to one or many multicast receivers over a network without requiring a multicast protocol, such as PIM, to be configured in the network.

You can apply a metric value to a dynamic LSP or a Point-to-Multipoint LSP that determines which LSP the 5620 SAM uses when multiple LSPs lead to the same destination. The metric value for a static route is set to 1 and cannot be configured.

You can list and view detailed information on LSPs, templates, cross connections, service tunnels, and detour and bypass information on the LSP (Edit) forms.

Dynamic LSPs

A dynamic LSP uses a signaling protocol such as LDP or RSVP-TE and an MPLS path between two NEs. You can then create an LSP between the two NEs and bind it to an MPLS path. An LSP-MPLS path binding is called an LSP path. You can configure the LSP path after the MPLS path and the LSP are bound.

Dynamic LSPs are categorized as follows:

- Explicit-path LSPs resemble static LSPs when all hops are strict; each hop in the LSP requires explicit configuration. MPLS uses RSVP-TE to set up an explicit-path LSP. Transit NE hops can be strict, and use a direct path between NEs, or loose, and include other NEs in the path between NEs.
- Constrained-path LSPs have dynamically assigned intermediate NE hops that rely on CSPF to find a path that satisfies the LSP constraints. CSPF is a routing algorithm that takes different LSP constraints, such as the available bandwidth and MPLS administrative groups, into account to balance the network load. When the CSPF path is found, RSVP uses the path to request the LSP setup. If Fast Reroute is enabled, the ingress NE signals the downstream NEs to set up a detour configuration for the LSP.

When an LSP is established, the reserved bandwidth is controlled by the bandwidth parameter at the primary path level, regardless of whether the LSP has auto-bandwidth enabled. When auto-bandwidth is enabled and a trigger occurs, the NE attempts to change the bandwidth of the LSP to a value between the minimum and maximum bandwidth, which are configurable at the LSP level. Automatic bandwidth allocation is supported on RSVP LSPs that have both CSPF and MBB enabled. If an RSVP LSP is configured for auto-bandwidth, the ingress LER determines, at every adjust interval, whether to attempt an auto-bandwidth adjustment. You can change the minimum bandwidth, maximum bandwidth, or threshold parameters on an operational LSP, however, the changes do not take effect until the next auto-bandwidth trigger, for example, an adjust interval expiry. If the bandwidth adjustment fails, for example, the CSPF cannot find a path, the existing LSP is maintained with its existing bandwidth reservation. See Procedure 25-8 for more information.

The 5620 SAM provides OAM tools for troubleshooting service and network transport issues. You can run an OAM validation test for the dynamic LSP by clicking on the One Time Validation button. If a check mark appears beside the OAM Validation Failed state cause indicator, the test has failed. The One Time Validation Result tab on the Tests tab displays detailed information about the OAM test result. See Procedure 77-9 for information on how to use the One Time Validation function.

Static LSPs

A static LSP uses an IGP instead of a signaling protocol, such as LDP or RSVP-TE. The 5620 SAM attempts to derive the hop configurations based on the hop labels in the path. You must use an ingress label that is unique within an NE when you create a new static hop; otherwise, the 5620 SAM rejects the new hop.

You can assign static label mappings for LSP cross-connections on an MPLS interface during interface creation or modification. A static label map is used only for intervening unmanaged NEs. The 5620 SAM attempts to derive the interface and label values from the swap egress label of the previous hop. The Static Label Maps form lists the static label maps for an interface whether they are created using the 5620 SAM client GUI, an OSS client, or CLI.

The 5620 SAM does not raise an alarm against an unmanaged NE.

The 5620 SAM raises an alarm against a static LSP under the following conditions when the LSP destination is managed by the 5620 SAM:

- No hops are configured for the static LSP.
- The last hop does not match the LSP destination.
- The label action specified for the last hop is not a pop action.

Point-to-Multipoint LSPs

A Point-to-Multipoint (P2MP) MPLS LSP allows the source of multicast traffic to forward packets to one or many multicast receivers over a network without requiring a multicast protocol, such as PIM, to be configured in the network. A P2MP LSP tree is established in the control plane for which the path consists of a head-end NE, one or many branch NEs, and multiple leaf NEs. Packets that are injected by the head-end NE are replicated in the data plane at the branching NEs before they are delivered to the leaf NEs.

The P2MP LSP has a source IP address but does not a have a destination address. Instead, you must create S2L leaf NEs for each destination in the P2MP LSP tree. The P2MP LSPs are not supported in SDP bindings.

Each P2MP LSP object has one P2MP LSP instance object. This is the primary instance, and can contain multiple child S2L path objects. Just as the P2MP LSP can appear as a tree, each S2L path object represents a root-to-leaf (S2L) sub-LSP path for the primary instance. The S2L paths can be empty paths or can specify a list of explicit hops. The same path can be used by more than one S2L of the instance. However the destination IP address must have a unique argument per S2L, because it corresponds to the address of the egress LER NE.

PIM tunnel interfaces are associated with a P2MP LSP. The tunnel interfaces are needed at both the ingress LER and the egress LER NEs. You must also associate static multicast groups with the tunnel interfaces that are associated with the P2MP LSPs.

On the ingress side, you can create one or more tunnel interfaces in PIM and associate each with a different RSVP P2MP LSP. The tunnel interface is associated with the P2MP LSP name. You can then assign static multicast group joins to each tunnel interface using an IGMP configuration. A specific <*,G> or <S,G> can only be associated with a single tunnel interface. A multicast packet which is received on an interface and matches the <*,G> or <S,G> specified in the IGMP join for the tunnel interface is replicated and forwarded to all branches of the P2MP LSP.

On the egress side, the PIM tunnel interface is associated with both the P2MP LSP name and the system address of the ingress LER. You must define a multicast info policy to associate specific multicast groups, or a specific <S,G>, to the primary tunnel interface on each egress LER leaf NE. The multicast info policy must then be applied to the router. A multicast packet synced from a tunnel interface associated with a P2MP LSP on the egress leaf NE can then be forwarded over a PIM or IGMP interface, which can be an access interface or a network interface, including a spoke SDP-based IES interface. You may create multiple tunnel interfaces per NE, where each interface is associated with a different P2MP LSP. The P2MP LSP association to a multicast group can be applied at the bundle, channel, and/or source channel level in the policy.

You can create a P2MP LSP using the LSP template for MVPN from the Policies→MPLS→LSP Template MVPN menu option. You can configure the scope as either local or global. The global template can be modified and multiple local versions can exist on the NEs. You must assign a default MPLS path to the template on the local definition before the template is turned up. If you modify the template, you must shut down the local policy first. When you turn up the local policy, all previously created P2MP LSP parameters are synchronized with the new template. See Procedure 25-23 for more information.

Bypass LSPs and manual bypass tunnels

You can create manual bypass tunnels and dynamic (or automatic) bypass tunnels on the SR/ESS, 7705 SAR, and 7210 SAS. You can manually configure an LSP to be bypass-only on a PLR NE. The LSP is then used exclusively for the purpose of bypass protection.

You can use manual bypass alone or with dynamic bypass. When used with the dynamic bypass, the manual bypass has precedence over the dynamic bypass for the path selection.

Dynamic bypass tunnels can be disabled on a per-NE basis. They are enabled by default. If dynamic bypass is disabled on a network element while dynamic bypass tunnels are active, traffic loss occurs. Furthermore, if no suitable manual bypass LSPs are found, the protected LSP remains without protection.

A bypass-only LSP does not have all the configurable attributes of a regular dynamic LSP. The main differences include:

- Manual bypass LSPs only support primary path. Secondary or standby paths cannot be created.
- Manual bypass LSPs do not support bandwidth or fast-reroute.
- Path monitoring is not available for manual bypass LSPs.
- Manual bypass LSPs cannot be assigned to a service tunnel, or be added to an LDP targeted peer as the LDP tunnelling LSP.
- There is no rule-based topology support available for manual bypass LSPs.
- There is no network-wide LSP view (the physical map LSP view) support available for manual bypass LSPs,
- You cannot create a static LSP using a tunnel template.

The following additional characteristics also apply to a manual bypass:

- The default protection level for a bypass tunnel is “node-protect”.
- CSPF is supported for the manual bypass tunnel. When CSPF is enabled, loose path and hop-less path are allowed on a manual bypass tunnel. The CSPF calculation is performed when the manual bypass tunnel is first set up.

Administrative groups with facility bypass backup LSPs

Administrative group constraints configured on an LSP primary path are used for signaling of bypass LSPs. The 5620 SAM supports P2P LSP and P2MP S2L path bypass LSPs. Administrative groups with one-to-one detour LSPs are not supported.

You can enable the use of administrative group constraints in the association of a manual or dynamic bypass LSP with the primary LSP path on the MPLS instance of the NE. When constraints are enabled, each PLR NE reads the constraints in the FAST_REROUTE object in the path message of the primary path LSP. If the FAST_REROUTE object is not included in the path message, the PLR NE reads the constraints from the session attribute object in the path message. The PLR NE uses the administrative group constraints and other constraints, such as the hop limit and SRLG, to choose a manual or dynamic bypass LSP from the LSPs that are in use.

You can enable the use of the administrative group constraints on FRR backup LSP on the P2P and the P2MP LSP configuration forms, and in the LSP template MVPN policy. The constraints apply only to new attempts to find a valid bypass.

Automatic ABR selection and dynamic ABR bypass protection

The ABR selection for the inter-area RSVP P2P LSP path computation by CSPF is automatic at the ingress LER. You do not need to include the ABR as a loose-hop in the LSP path definition. On the LSP path binding configuration form, you can view whether:

- the operational path is inter-area or intra-area
- the current CSPF hop is an ABR (on the CSPF Path tab)

Dynamic bypass LSP for ABR NE protection

The 5620 SAM provides dynamic bypass computation, signaling, and association with the primary path of an inter-area P2P LSP to provide ABR NE protection. For a PLR NE within the local area of the ingress LER to provide ABR NE protection, the NE must dynamically signal a bypass LSP and associate it with the primary path of the inter-area LSP. You can view the address of the NE that must be bypassed along the path in the RSVP session tab on the dynamic LSP properties form.

Tunnel Templates

Tunnel templates allow users to configure dynamic LSP, LSP path, and SDP templates to define common characteristics for a tunnel or templatable tunnel object. Configure tunnel templates to reduce configuration time. See "XML API template administration" in the *5620 SAM Scripts and Templates Developer Guide* for information about creating tunnel XML API templates.

To simplify creating tunnel templates, the 5620 SAM provides examples of common tunnel templates that can be copied and customized. You can also create a tunnel template from an existing templatable object.

After a template is configured, dynamic LSPs, LSP paths and SDPs can be configured by choosing a create from template button during configuration. Users can configure multiple LSP paths for a dynamic LSP. For example, you can configure one primary, one standby, and many secondary LSP paths.

When the 5620 SAM auto-tunnel creation is used to create LSP paths, the LSP paths must use a hopless path. If the paths belong to the same LSP, they must use different MPLS paths, even when the MPLS paths are hopless. For a RSVP LSP policy, one LSP template can be specified. When an LSP template with multiple LSP paths is specified, many LSP paths are created.

LSP Path Optimization Policy

The 5620 SAM allows you to resignal LSP Paths to take advantage of new paths that are less congested, fewer hops, have a lower metric and meet least-fill criteria. NEs periodically check the network to determine whether a more efficient path is available and notify the 5620 SAM when another path is eligible for re-signalling. 5620 SAM maintains a list of LSP Paths that are eligible for re-signaling. When a LSP Path is eligible for optimization, the LSP Path can be routed to a different path. When a LSP Path not eligible for optimization, the LSP Path cannot use newly available network resources.

A LSP Path optimization policy allows the operator to filter the LSP Path candidates and set the execution rules to determine the candidacy and priority of an LSP Path for re signalling. The 5620 SAM operator can define LSPs Paths that are eligible for re-signaling and if a path is selected, the LSP Path is added to a candidate list. Execution rules determine the sequence in which the LSP Paths can re-signal and the number of seconds between re-signalling. Execution rules apply to the entire candidate list. Each time that optimization starts, the candidate list is filtered according to the candidate definition values and then re sequenced according to the sequencing target and order values.

To ensure that NEs are not overloaded by LSP re-signaling, an LSP Path optimization schedule can be created to identify when re-signaling can be evaluated and executed. You can also manually execute LSP Path optimization schedules. To avoid network congestion and maintain QoS standards, one policy should be executed at a time. Repetitive re-signaling requests are ignored, including manual or scheduled re-signaling requests. However, a re-signaling request that is initiated from the LSP Path binding properties form executes regardless of whether another LSP optimization policy is in progress.

The NEs notify the 5620 SAM about the current state and outcome of LSP Path re-signaling. You can access the LSP Path property form to view information about the state of LSP Path optimization. The following parameters are displayed:

- The Resignal Eligible parameter indicates whether a LSP Path is eligible for optimization. When the parameter value is true, the LSP Path can be optimized. When the parameter value is false, the LSP Path is not eligible for optimization.
- The Last Performed Type parameter indicates how resignaling was performed. Typically the value is Manual Resignal. However, if a schedule was set, the value is Timer Based Resignal.
- The Last Performed parameter indicates the last time the LSP Path was chosen to be re-signaled.
- The Last Performed State parameter indicates the re-signal state of a specific LSP Path.

LDP-over-RSVP tunnels

In networks that contain dozens of NEs spanning multiple routing areas, many RSVP service tunnels may be required. To reduce the number of RSVP tunnels required for service deployment in large networks, you can use the 5620 SAM to create LSPs using LDP-over-RSVP, sometimes called tunnel-in-tunnel encapsulation. An SDP can ride on multiple LDP-over-RSVP tunnels.

The 5620 SAM supports automatic, rule-based service-tunnel creation using NEs that are grouped according to their role in the 5620 SAM-managed network. This functionality greatly reduces the time and effort required to provision a mesh of service tunnels. See chapter 27 for more information about rule-based automatic service-tunnel creation.

The 5620 SAM can use tunnel rules and groups to create new RSVP LSP bindings between a PE device that is added to the network and the existing ABRs. It can also create a new LDP-over-RSVP tunnel between a new NE and an existing PE NE. See chapter 27 for more information about tunnel creation using rules and groups.

Service traffic that is transported by an LDP-over-RSVP tunnel requires a VC label, an LDP label, and an RSVP label. Unlike T-LDP sessions that use IGP SPF algorithms, RSVP LSPs are not advertised to an IGP instance. When the same FEC applies to the destination of an LDP-over-RSVP LSP tunnel and an IGP-based LDP tunnel, the 5620 SAM uses the LDP tunnel by default to minimize network overhead.

Using tunnel-in-tunnel encapsulation, a pair of LSP tunnels and a T-LDP session between two NEs are equivalent to two adjacent LDP NEs with a non-tunneled LDP session between them. In other words, the LDP tunnel uses the RSVP LSP as one hop between LSRs in the network.

During the configuration of LDP-over-RSVP, you can specify an explicit list of dynamic and static LSPs, or use the 5620 SAM to find eligible LSPs. After an LSP is explicitly configured for LDP tunnelling, the 5620 SAM associates the LDP targeted peer with the LSP.

You can configure LDP-over-RSVP to enable an OSPF area router to be a stitching point. You can specify which NEs to use as the stitching points in each area. When there are many NEs in an area, this function helps to reduce the number of LSPs required, because a full mesh is not required.

For an LSP to be eligible for LDP-over-RSVP, the following conditions apply:

- The LSP must be an RSVP-owned LSP (strict or loose)
- The LSP must start and terminate either on:
  - The router ID (system IP address)
  - The router ID (loopback address when used in multi-instance OSPF
- The OSPF system/loopback address must be advertised
- A T-LDP session must exist between the originating and terminating routers using the addresses cited above
- LDP-over-RSVP availability must be enabled in the LSP configuration. This indicates that the LSP is eligible for LDP-over-RSVP, and RSVP signals to the IGP that the LSP should be included in the SPF run.

Shared Risk Link Groups

Shared Risk Link Groups, or SRLGs, are constructs which allow you to perform two operations that enhance overall system reliability. Firstly, you can establish a FRR LSP path. In addition, you can also use SRLGs to establish a secondary LSP path which is disjointed from the primary LSP path.

Configured SRLGs are associated with MPLS interfaces. The SRLGs are used by the CSPF when computing a FRR detour/bypass path, or a secondary LSP path. Links which are members of the same SRLG represent resources which are assumed to share the same risk. These links are therefore avoided when computing and setting up an alternate LSP path.

- FRR backup

  The SRLG constraint can be enabled system-wide on a PLR NE, in the computation of a FRR detour or bypass to be associated with a primary LSP path. CSPF includes the SRLG constraint in the computation of a FRR detour or bypass. CSPF then prunes all links with interfaces which belong to the same SRLGs as the egress interface being protected (or the immediate downstream NE, depending on the protection level). If a path is found, the bypass or detour is set up. If not, and you included the Enable SRLG for FRR - Strict option, then the bypass or detour is not set up. If the Enable SRLG for FRR - Strict option is not specified, and a path exists that meets other TE constraints (other than the SRLG constraint), then the bypass or detour is still set up.
- Secondary LSP backup

  The SRLG constraint can also be enabled per LSP path on a head-end LER in the computation of an LSP secondary path that includes the standby path. The SRLG constraint is additional to the admin group constraint on the same secondary LSP path. CSPF includes the SRLG constraint in the computation of the secondary LSP path, which requires that the primary LSP path is configured and active.

CSPF prunes links with interfaces that belong to the same SRLGs as the interfaces included in the primary path. If a path is found, the secondary LSP path is set up. Otherwise, CSPF keeps trying to set up the secondary LSP path.

You can enable only the SRLG constraint for the FRR backup operation. However, you can enable both the SRLG constraint and the admin-group include/exclude constraint for the secondary LSP backup path operation. In either case, you can still apply the admin-group constraint for the primary path.

The following conditions also apply to SRLGs:

- An SRLG is modeled as a policy object. It therefore follows the normal policy behavior for creation, listing, updating, deletion, distribution and resynchronization
- SRLGs are defined node-wide
- Configured SRLGs are associated with MPLS interfaces. A specific MPLS interface can belong to multiple SRLGs. Up to 64 SRLGs can be associated with a specific MLPLS interface

Bandwidth-based equal cost RSVP LSP path selection

When multiple equal-cost paths satisfy the constraints of a specific RSVP LSP path, CSPF in the 7x50 head-end NE uses a random number generator to choose a path and return it to MPLS. While this method actually balances the number of LSP paths over the links in the network, it does not necessarily balance the bandwidth utilization across those links.

In order to achieve load balancing of the bandwidth amongst the available LSP paths, CSPF must include the link utilization as a criterion in the path selection. One algorithm that considers this is referred to as the “least-fill” path selection. This algorithm identifies the single link in each of the equal-cost paths that has the least available bandwidth in proportion to its maximum reservable bandwidth. CSPF then selects the path containing the link with the largest such available bandwidth to maximum reservable bandwidth percentage. The net effect of using this algorithm is that over time, LSP paths become spread over the network links in such a way that the percentage of link utilization is balanced.

When comparing the percentages of least available link bandwidth across the sorted paths, if two percentages differ by less than a value you configure as a minimum threshold, CSPF considers them equal. It then applies a random number generator to choose amongst these paths. You can also specify a reoptimization threshold, which allows you include a path cost consideration into the decision of when to alter the paths used by the LSP.

LSP on-demand resynchronization

LSP on-demand resynchronization is supported on the 7750 SR, 7710 SR, and 7950 XRS. On-demand resynchronization does not affect the existing manual full NE resynchronization functionality. However, when LSP on-demand resynchronization is enabled, any scheduled resynchronization is blocked for the following LSP objects:

- RSVP session
- cross-connect
- in-segment
- out-segment
- actual hop
- CSPF hop

Therefore, these LSP objects are not resynchronized as a result of a relevant trap. The exception is that for 5650 CPAM path monitored LSPs, the actual hop trap (a generic trap) is still processed.

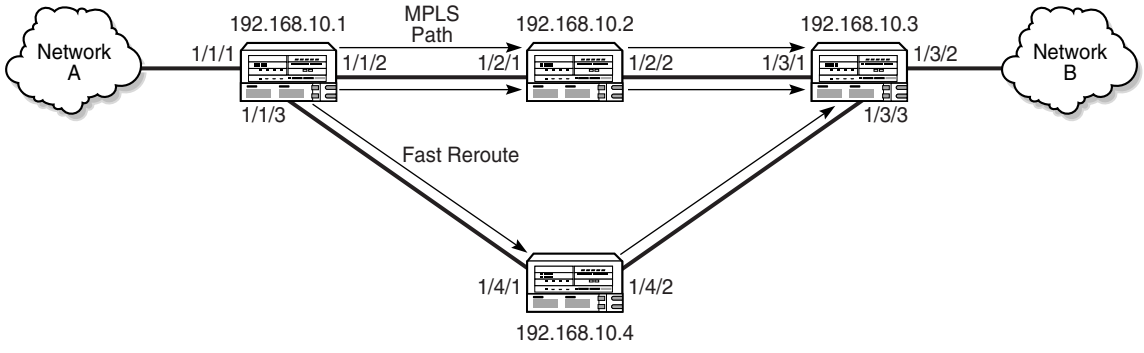
By default, the LSP on-demand resynchronization functionality is disabled. See "To enable LSP on-demand resynchronization" in the *5620 SAM System Administrator Guide* for more information. After you enable LSP on-demand resynchronization, click on the Resync button on the LSP configure form to start the manual LSP on-demand resynchronization. The following objects are resynchronized, depending on the type of LSP:

- for a dynamic LSP: the LSP, LSP path, CSPF and actual paths, bypass or detour path, cross-connects, in-segments, out-segments, and RSVP sessions
- for a manual bypass LSP: the LSP, LSP path, CSPF and actual paths, cross-connects, in-segments, out-segments, and RSVP sessions
- for a static LSP: the head-end LSP, the static hops, static label maps, cross-connects, in-segments, and out-segments. You must manually resynchronize all of the planned hop sites in a static LSP before creating a static LSP.

25.2 Sample MPLS configuration

Figure 25-1 shows an example of an MPLS service configuration. The actual configuration depends on the specific network requirements.

Figure 25-1 Sample MPLS configuration



The high-level tasks that are required to configure the MPLS service example in Figure 25-1 follow.

Preconfiguration

1 Before you begin, verify that the following preconfigurations have been made.

- An IGP is enabled on all participating NEs and includes the system interface in the IS-IS or OSPF area.
- Any additional Layer 3 interfaces that you wish to use are configured.

Configuration

2 Create an MPLS path as follows:

i Specify 192.168.10.1 as the source network element.

ii Specify 192.168.10.2 and 192.168.10.4 as hops.

iii Specify interface 1/3/2 on 192.168.10.3 as the destination site. This is the final hop in the MPLS path.

3 Create a dynamic LSP as follows:

i Specify interface 1/1/1 on 192.168.10.1 as the source IP address.

ii Specify 192.168.10.3 as the destination IP address.

4 Bind the dynamic LSP created in step 3 to the MPLS path created step 2.

25.3 Workflow to configure MPLS

1 Enable and configure one or more IGPs such as IS-IS, RIP, and OSPF to include the system interface on all NEs that are to participate in the MPLS network. See the appropriate device documentation for more information.

2 Enable MPLS on the routing instances of all NEs that are to participate in the MPLS network. See Procedure 25-1.

3 Create or configure an MPLS instance. Assign Layer 3 interfaces, including the system management interface, to the MPLS instance. See Procedure 25-2 or 25-3.

4 Create a mesh of MPLS paths. See Procedure 25-4.

5 As required, create a mesh of LSPs.

a Create a static LSP. See Procedure 25-6.

b Create a dynamic LSP. See Procedure 25-8. See Procedure 25-10 for more information about how to create a dynamic LSP from a tunnel template.

c Create a Point-to-Multipoint LSP. See Procedure 25-13.

d Create a Manual Bypass LSP. See Procedure 25-14.

6 If your mesh includes dynamic LSPs or bypass-only LSPs, configure an LSP path. See Procedure 25-16 or 25-17.

7 Create an LSP Path optimization policy, if required. See Procedure 25-18.



Note 1 — Only static LSPs and static FRR LSPs are supported on the OS 9700E and OS 9800E NEs.

Note 2 — RSVP is not supported on the OS 9700E and OS 9800E NEs.

Note 3 — Label actions cannot be modified on NEs after the labels are created by the 5620 SAM.

25.4 MPLS procedures

Use the following 5620 SAM procedures to manage MPLS.

Procedure 25-1 To enable MPLS on a routing instance

1 Choose Routing from the 5620 SAM navigation tree view selector.

2 Navigate to a routing instance. The path is Routing→NE→Routing Instance.

3 Right-click on the routing instance and choose Properties from the contextual menu. The Routing Instance (Edit) form opens.

4 Click on the Protocols tab.

5 Enable the MPLS Enabled parameter. RSVP is enabled by default and cannot be disabled using the 5620 SAM.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The Routing Instance (Edit) form closes. The 5620 SAM creates an MPLS instance and displays the instance below the routing instance in the navigation tree.

Procedure 25-2 To configure an MPLS instance



Note — The following tabs are supported on the OS 9700E and OS 9800E NEs for MPLS configuration at the site level:

- General
- Interfaces
- In Segments
- Cross Connects
- Out Segments
- Static Label Maps
- Faults

1 Enable MPLS on an NE, as described in Procedure 25-1.

2 Choose Routing from the 5620 SAM navigation tree view selector.

3 Navigate to an MPLS instance. The path is Routing→NE→Routing Instance→MPLS.

4 Right-click on the MPLS icon in the navigation tree, and choose Properties from the contextual menu. The MPLS (Edit) form opens with the General tab displayed.

5 Configure the Administrative State parameter in the States panel.

6 Configure the parameters in the Configuration panel:

- Fast Reroute Signaling
- Dynamic Bypass
- Exponential Backoff Retry
- Logger Event Bundling
- Enable Administrative Group for FRR Path Computation
- Static LSPs Fast Retry Timer (seconds)
- Secondary Fast Retry Timer (seconds)
- Static LSPs Fast Retry Timer (seconds)
- Maximum Bypass Associations
- Maximum Number of Static LSP Labels
- Maximum Number of Static SVC Labels

7 Configure the parameters in the LSP Resignal panel:

- Enable
- Resignal Timer (min)
- Active Path Fast Retry Timer (seconds)

8 Configure the parameters in the P2MP LSP Resignal panel:

- Enable
- Resignal Timer (min)
- S2L Active Path Fast Retry Timer (seconds)

9 Configure the Hold Timer (seconds) parameter in the Hold Timer panel.

10 Configure the parameters in the Shared Risk Link Group panel:

- Enable SRLG for FRR
- Strict
- Use SRLG Static Configuration

11 Configure the parameters in the Least-Fill panel:

- Least Minimum Threshold
- Least Reoptimization Threshold

12 Configure the parameters in the TTL Propagate panel:

- Shortcut Local TTL Propagate
- Shortcut Transit TTL Propagate

13 Configure the parameters in the Auto Bandwidth Multipliers panel:

- Sample Multiplier
- Adjust Multiplier

14 Configure the CSPF On Loose Hop parameter in the Inter Area/Level Traffic Engineering panel.

15 If you need to configure OAM diagnostics for the MPLS instance, click on the Tests tab. See chapter 32 for more information about how to configure OAM diagnostics.

16 To configure MPLS interfaces on the MPLS instance, click on the Interfaces tab. See Procedure 25-3 for more information about how to configure MPLS interfaces.

17 To configure the collection of ingress accounting statistics for the MPLS instance, click on the Accounting tab.

18 Click on the Create button. The IngStatsPolicy, Routing Instance (Create) form opens.

19 Configure the parameters in the LSP Information panel:

- LSP Name
- Sender Address

20 Configure the parameters in the Ingress Accounting Statistics panel:

- Click on the Select button. The Select Accounting Policy - IngStatsPolicy - Routing Instance form opens. Choose the required accounting policy and click on OK. Only accounting policies with the CombinedMplsLspIngressStats stats type are available for selection.
- Collect Accounting Statistics
- Administrative State



Note — The collection of egress accounting statistics is configured in Procedure 25-8.

See “Statistics collection overview” in the *5620 SAM Statistics Management Guide* for more information on the collection of statistics.

21 Click on the following tabs to view information about the MPLS instance, as required.

- In Segments to view the MPLS ingress segment information, such as label assignments
- Cross Connects to vie w the LSP cross-connection information
- Out Segments to view the MPLS egress segment information, such as label assignments
- Static Label Maps to view static hop mapping information
- Statistics to view MPLS site and interface statistics
- Faults to view alarm information for the MPLS instance

22 Click on the View RSVP Site button to view the associated RSVP instance on the NE. If the View RSVP Site button is not visible, click on the More Actions button and choose View RSVP Site.

23 Click on the OK button. A dialog box appears.

24 Click on the Yes button. The MPLS (Edit) form closes.

Procedure 25-3 To create an MPLS interface

Perform this procedure to create an MPLS interface by assigning a network interface to an MPLS instance.

This procedure requires the existence of a numbered or unnumbered L3 network interface on the NE that hosts the MPLS instance. See section 22.1 for more information about how to configure network interfaces.



Note — The following tabs are supported on the OS 9700E and OS 9800E NEs for MPLS configuration at the interface level:

- General
- In Segments
- Static Label Maps
- Cross Connects
- Out Segments
- Faults

1 Choose Routing from the 5620 SAM navigation tree view selector.

2 Navigate to an MPLS instance icon. The path is Routing→NE→Routing Instance→MPLS.

3 Right-click on the MPLS icon and choose Create Interface from the contextual menu. The MPLS Interface (Create) form opens with the General tab displayed.

4 Assign a numbered or unnumbered L3 network interface as the MPLS interface.

i Click on the Select button. The Select Interface form opens.

ii Choose an interface from the list and click on the OK button.The interface is displayed in the Interface panel on the MPLS Interface (Create) form.

5 Configure the parameters:

- Description
- Administrative State

6 In the TE Metric panel, configure the parameters:

- TE Metric Enabled
- TE Metric

7 Click on the Apply button. The form displays additional tabs, and the 5620 SAM creates the MPLS interface and displays it below the MPLS and RSVP instances in the navigation tree.

8 Configure a Shared Risk Link Group, if required.

i Click on the Shared Risk Link Groups tab. The Shared Risk Link Group list page opens.

ii Click on the Create button. The SharedRiskLinkGroup (Path/Routing Management: MPLS) Select form opens.

iii Click on the Search button. The available SRLGs are displayed.

iv Select the required SRLGs and click OK. Up to 64 SRLGs can be associated with a specific MPLS interface. The SharedRiskLinkGroup (Path/Routing Management: MPLS) Select form closes and the selected SRLG is displayed in the Shared Risk Link Group list page.

9 Configure a static label map, if required. A static label map is required when there are intervening unmanaged NEs between the managed NEs in an MPLS path.



Note — Alcatel-Lucent recommends that you use a static label mapping only to specify unmanaged NEs.

i Click on the Static Label Maps tab.

ii Click on the Create button. The Static Label Map (Create) form opens. Alternatively, you can choose a Static Label Map from the list and click on the Properties button to edit the Static Label Map properties.

iii Configure the Label Action parameter. When you change the Label Action parameter from unspecified to Pop or Swap, the Static Label Map (Create) form changes to include other parameters. Configure the other parameters as required:

- Ingress Label
- Egress Label
- Egress Label
- Enable Implicit Null Label
- Next Hop
- Next Hop
- Administrative State

The Egress Label, Next Hop and Enable Implicit Null Label parameters are only configurable when the Label Action parameter value is set to Swap.

The Egress Label and Next Hop parameters are configurable only when the Label Action parameter value is set to Swap/Protect-Swap.

The 5620 SAM sets the Label Action parameter value to Pop when the hop destination matches the destination LSP.

iv Click on the OK button. A dialog box appears.

v Click on the OK button.

10 Click on the Administrative Groups tab to assign MPLS administrative groups to the interface, as required. After you assign administrative groups to an MPLS interface, the total value of the groups is displayed in a bit mask format by the Groups Included (bitmask) indicator on the General tab.

11 Click on the following tabs to view information about the MPLS interface, as required.

- In Segments to view the MPLS ingress segment information, such as label assignments
- Cross Connects to vie w the LSP cross-connection information
- Out Segments to view the MPLS egress segment information, such as label assignments
- Statistics to view the MPLS site and interface statistics
- Faults to view alarm information for the MPLS interface

12 Click on the OK button. A dialog box appears.

13 Click on the Yes button. The MPLS Interface properties form closes.

Procedure 25-4 To create an MPLS path

1 Choose Manage→MPLS→MPLS Paths from the 5620 SAM main menu. The Manage MPLS Paths form opens.

2 Click on the Create button. The Create MPLS Path form opens with the Name the MPLS Path step displayed.

3 Configure the parameters:

- Name
- Description

4 Click on the Next button. The Define Source Site step displayed.

5 Perform one of the following actions to specify a 5620 SAM-managed NE for the Starting Network Element parameter value.

a Choose an NE from a list.

i Click on the Select button. The Select a Network Element - Select Source Site form opens.

ii Choose an NE and click on the OK button. The management IP address of the NE is displayed as the source site of the MPLS path.

b Enter the management IP address of the port.

6 Click on the Next button. The Define the provisioned Path step is displayed.

7 Click on the Insert Hop button to insert an MPLS path hop. The Hop for New MPLS Path (Create) form opens.

8 Configure the Specify Site parameter. Perform one of the following actions.

a Specify the IP address of an unmanaged NE.

i Choose Manually.

ii Configure the IP Address parameter.

b Choose a managed NE.

i Choose By Selection.

ii Click on the Select button. The Select a Network Element - New MPLS Path form opens.

iii Choose an NE and click on the OK button. The management IP address of the NE is displayed as the IP Address value.

iv Specify an alternative or loopback (only for Dynamic P2P RSVP LSPs) interface on the NE to be used as the hop point, if required. Otherwise, go to step 9.

v Click on the IP Address parameter Select button. The Select a Virtual Router Interface form opens with a list of the available interfaces.

vi Choose an interface and click on the OK button. The Select a Virtual Router Interface form closes and the Hop for New MPLS Path (Create) form displays the IP Address of the selected loopback interface.

9 Configure the Hop Type parameter.

10 Click on the Apply button.

11 Insert an additional hop, if required, by repeating steps 8 to 10.

12 Click on the OK button. The Create MPLS Path form reappears.

13 To change the hop sequence, choose a hop and click the Move Up or Move Down button. The first hop in the list is the first hop, and the last hop becomes the destination site when the form changes are saved.

14 Click on the Next button. The Set Initial State step is displayed.

15 Configure the Administrative parameter.

16 Click on the Finish Button to save the configuration. You are prompted to view the MPLS path.

17 Enable the View the newly created MPLS path parameter to view the MPLS path configuration after closing the form, if required.

18 Click on the Close button. The Create MPLS Path form closes.

19 If the View the newly created MPLS path parameter in step 16 is enabled, the MPLS Path (Edit) form opens with the newly created MPLS path configuration displayed.

i View the configuration, if required.

ii Close the MPLS Path (Edit) form.

20 Close the Manage MPLS Paths form.

Procedure 25-5 To view an MPLS path

1 Choose Manage→MPLS→MPLS Paths from the 5620 SAM main menu. The Manage MPLS Paths form opens.

2 Configure the filter criteria. A list of MPLS paths is displayed.

3 View the MPLS path information as required. The information includes the following:

- name and description
- ID
- source and destination sites
- administrative and operational states

Procedure 25-6 To create a static LSP



Note — When LSP on-demand resynchronization is enabled, manually resynchronize all of the planned hops in the static LSP before you create a static LSP. This is to ensure that validations on the static LSP can be run properly. See "To enable LSP on-demand resynchronization" in the *5620 SAM System Administrator Guide* for more information.

1 Choose Manage→MPLS→Static LSPs from the 5620 SAM main menu. The Manage Static LSPs form opens.

2 Click on the Create button. The Static LSP (Create) form opens.

3 Configure the parameters:

- Name
- Description
- ID
- Auto-Assign ID
- Source Site ID
- Egress Label
- Enable Implicit Null Label
- Next Hop
- Administrative
- Destination Site ID



Note 1 — If a range policy is applied to a service tunnel, a grey text box appears beside the Service ID parameter to indicate that a range policy is in effect.

If a format policy is applied to a service tunnel, a combo box appears beside the object field during object creation, to indicate that a format policy is enforced. When there is only one matching policy, the combo box is dimmed. When there are multiple matching policies, the combo box is used to choose a policy. The items in the combo box are ordered by the policy's Priority parameter.

Note 2 — The Administrative parameter applies to the source NE only, not to the entire static LSP

4 Click on the Static Hops tab.

5 Click on the Create button. The Static Hop (Create) form opens.

6 Configure the Hop Index parameter.

7 Click on the Select button in the Site panel to configure the Site ID parameter. The Select Site - Static Hop form opens with a list of the available hop sites.

8 Choose a site and click on the OK button. The Select Site - Static Hop form closes and the Static Hop (Create) form displays the site information.

9 Click on the Select button in the Interface panel to configure the Interface Name parameter. The Select Interface - Static Hop form opens with a list of the available interfaces on the hop site.

10 Choose an interface and click on the OK button. The Select Interface - Static Hop form closes and the Static Hop (Create) form displays the interface name.

11 Configure the parameters:

- Label Action
- Ingress Label
- Egress Label
- Egress Label
- Enable Implicit Null Label
- Next Hop
- Next Hop
- Administrative State

The Egress Label, Enable Implicit Null Label and Next Hop parameters are configurable when the Label Action parameter value is set to Swap.

The Egress Label and Next Hop parameters are configurable only when the Label Action parameter value is set to Swap/Protect-Swap.

12 Click on the OK button. The Static Hop (Create) form closes and a dialog box appears.

13 Click on the OK button. Static LSP (Create) form reappears.

14 Insert an additional hop, if required, by repeating steps 5 and 13.

15 Click on the OK button. The Static LSP (Create) form closes and a dialog box appears.

16 Click on the Yes button. The Static LSP (Create) form closes and the Manage Static LSPs form reappears.

17 Close the Manage Static LSPs form.

Procedure 25-7 To view and configure a static LSP

The following procedure applies only to the 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7450 ESS, 7750 SR, 7710 SR, and 7950 XRS.

1 Choose Manage→MPLS→Static LSPs from the 5620 SAM main menu. The Manage Static LSPs form opens.

2 Configure the filter criteria and click on the Search button. A list of static LSPs is displayed.

3 Choose an LSP and click on the Properties button. The Static LSP (Edit) form opens.

4 Click on the following tabs to view information about the static LSP, as required.

- Static Hops to view and configure LSP hops
- Service Tunnels to view a list of service tunnels associated with the static LSP
- LDP Tunneling to view a list of LDP-over-RSVP tunnels associated with the static LSP
- Statistics to view the static LSP site and interface statistics
- Faults to view alarm information for the static LSP

5 Close the Static LSP (Edit) form.

6 Close the Manage Static LSPs form.

Procedure 25-8 To create a dynamic LSP

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form opens.

2 Click on the Create button. The Create Dynamic LSP step form opens with the Identification step displayed.

3 Configure the parameters:

- Name
- Description
- ID
- Auto-Assign ID
- Preference



Note — When a range policy is applied to a dynamic LSP, a dimmed text field appears beside the Service ID parameter to indicate that a range policy is in effect.

If a format policy is applied to a dynamic LSP, a combo box appears beside the object field during object creation, to indicate that a format policy is in effect. When there is only one matching policy, the combo box is dimmed. When there are multiple matching policies, the combo box is used to choose a policy. The sequence of the options in the combo box are specified by the policy Priority parameter.

4 Click on the Next button. The Define Source and Destination Sites step is displayed.

5 Specify the source and destination sites for the dynamic LSP.



Note — You can also manually specify an IP address for each parameter in the step.

i Click on the Source Site ID parameter Select button. The Select a Network Element - Create Dynamic LSP form opens with a list of the available sites.

ii Choose a site and click on the OK button. The Select a Network Element - Create Dynamic LSP form closes and the Create Dynamic LSP form displays the source site information, which includes the system Source IP Address parameter value. The parameter is automatically populated with the system IP address of the site.

iii If you are creating a P2P RSVP LSP, you can alternatively configure a loopback interface other than the system interface. Otherwise, go to step vi.

iv Click on the Source IP Address parameter Select button. The Select a Virtual Router Interface form opens with a list of the available interfaces.

v Choose an interface and click on the OK button. The Select a Virtual Router Interface form closes and the Create Dynamic LSP form displays the Source IP Address and Source Interface Name information of the selected loopback interface.

vi Click on the Destination Site ID parameter Select button. The Select a Network Element - Create Dynamic LSP form opens with a list of the available sites.

vii Choose a site and click on the OK button. The Select a Network Element - Create Dynamic LSP form closes and the Create Dynamic LSP form displays the destination site information. The default displayed destination interface is the system interface.

viii If you are creating a P2P RSVP LSP, you can alternatively configure a loopback interface other than the system interface as the destination. Otherwise, go to step 6.

ix Click on the Destination IP Address parameter Select button. The Select a Virtual Router Interface form opens with a list of the available interfaces.

x Choose an interface and click on the OK button. The Select a Virtual Router Interface form closes and the Create Dynamic LSP form displays the Destination IP Address and Destination Interface Name information of the selected loopback interface.

6 Click on the Next button. The Auto Select Hop-Less MPLS Path step form opens.

7 Configure the parameters:

- Auto Select Hop-less Path
- Reserved Bandwidth (Mbps)

The Reserved Bandwidth (Mbps) parameter is configurable when the Auto Select Hop-less Path parameter is enabled.

8 If the Auto Select Hop-less Path parameter in step 7 is enabled, go to step 10.

9 Click on the Next button. The Add MPLS Paths form opens. This step binds the LSP to the MPLS path to create an MPLS path.

i Configure the Path Destination Matching parameter.

ii Click on the Create button. The LSP-Path Binding form opens with the Choose Path Type step displayed.

iii Configure the Type parameter.

iv Click on the Next button. The Choose MPLS Path step is displayed.

v Choose an MPLS path to associate with the LSP. You can also create an MPLS path by clicking on the Create MPLS Path button. See Procedure 25-4 for more information.

vi Click on the Next button. The Set Traffic Options form opens.

vii Configure the parameters:

- Reserved Bandwidth (Mbps)
- Hop Limit
- Inherit Value
- Record Actual Path
- Path Preference

The Path Preference is only configurable on Standby LSP paths (Type parameter set to standby).

viii Click on the Next button. The Set Initial States form opens.

ix Configure the Administrative parameter.

x Click on the Finish button. The LSP-Path Binding form closes and a dialog box appears.

xi Click on the OK button. The Create Dynamic LSP step form reappears.

10 Click on the Next button. The Properties - Traffic Engineering and Protection step is displayed.

11 Configure the parameters:

- Fast Reroute
- Hop Limit
- IGP Shortcut Enabled
- BGP RSVP LSP Transport Tunnel
- BGP Shortcut Enabled
- Diff-Serv Class Type
- Main Class Type Retry Limit

12 Click on the Next button. The Properties - IGP Shortcut step is displayed.

13 Configure the parameters:

- LFA Type
- Relative Metric

14 Click on the Next button. The Properties - Fast Reroute step is displayed.

15 Configure the parameters:

- Backup Type
- Hop Limit
- Reserved Bandwidth (Mbps)
- Node Protect
- Propagate Administrative Groups

16 Click on the Next button. The Properties - Signalling step is displayed.

17 Configure the parameters:

- Retry Timer (seconds)
- Retry Limit
- RSVP Reserve Style
- Include ADSPEC in RSVP
- Propagate Administrative Groups via Session Attribute Object

18 Click on the Next button. The Properties - Make before Break step is displayed.

19 Configure the Make before Break parameter.

20 Click on the Next button. The Properties - CSPF form opens.

21 In the CSPF panel, configure the parameters:

- Enable CSPF
- Enable TE Metric

22 Click on the Next button. The Properties - Route Selection step is displayed.

23 Configure the parameters:

- Metric
- Least-Fill Path Selection

The Least-Fill Path Selection parameter can only be enabled when the Enable CSPF parameter is enabled in step 21.

24 Click on the Next button. The Properties - Administrative Groups step is displayed.

25 Assign one or more MPLS administrative groups to the dynamic LSP.

i Select the required MPLS administrative groups in the Unassigned list.

ii Click on the right arrow button. The groups are assigned to the dynamic LSP and moved to the Assigned list.

After you assign administrative groups to an MPLS interface, the total value of the groups is displayed in a bit mask format by the Groups Included (bitmask) indicator on the General tab.

26 Click on the Next button. The Properties - LDP Tunneling step is displayed.

27 Configure the LDP over RSVP include parameter.

28 Click on the Next button. The Properties - Auto-Bind step is displayed.

29 Configure the Enable Auto-Bind parameter.



Note — The Enable Auto-Bind parameter is configurable only on a 7710 SR, 7750 SR, or 7950 XRS.

30 Click on the Next button. The Set Initial State step is displayed.

31 Configure the Administrative parameter.

32 Click on the Finish button. The 5620 SAM prompts you to view the dynamic LSP.

33 Enable the View the newly created Dynamic LSP parameter to view the dynamic LSP configuration after closing the form, if required.



Note — If you enable the View the newly created Dynamic Lsp parameter you can configure the collection of egress accounting statistics using the dynamic LSP configuration form.

34 Click on the Close button. The Create Dynamic LSP form closes.

35 If the View the newly created Dynamic LSP parameter is enabled in step 33, the Dynamic LSP (Edit) form opens with the newly created dynamic LSP configuration displayed.

i View the configuration, if required.

ii If you need to enable the collection of egress accounting statistics, go to step iii. Otherwise go to step v.

iii Click on the Accounting tab.

iv Configure the parameters in the Egress Accounting Statistics panel:

- Click on the Select button. The Select Accounting Policy - Dynamic LSP form opens. Choose the required accounting policy and click on the OK button. Only accounting policies with the CombinedMplsLspEgressStats stats type are available for selection.
- Collect Accounting Statistics
- Administrative State



Note 1 — The Ingress Accounting Statistics panel displays a read-only view. If an ingress accounting statistics record exists, you can click on the Properties button to view the record.

Note 2 — The collection of ingress accounting statistics is configured in Procedure 25-2.

See “Statistics collection overview” in the 5620 SAM Statistics Management Guide for more information on about the collection of statistics.

v Click on OK to close the Dynamic LSP (Edit) form.

36 Click on OK to close the Manage Dynamic LSPs form.

Procedure 25-9 To configure a dynamic LSP

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form opens.

2 Click on the Search button. A list of dynamic LSPs is displayed.

3 Choose a dynamic LSP from the list and click on the Properties button. The Dynamic LSP (Edit) form opens with the General tab displayed.

4 Configure the Description parameter.

5 Configure the Administrative parameter in the States panel.

6 Click on the Properties tab button.

7 Configure the parameters in the Traffic Engineering Properties panel:

- Fast Reroute
- Hop Limit
- BGP RSVP LSP Transport Tunnel
- IGP Shortcut Enabled
- BGP Shortcut Enabled
- Diff-Serv Class Type
- Main Class Type Retry Limit
- Auto Bandwidth

8 If you enabled the IGP Shortcut Enabled parameter in step 7, configure the parameters in the IGP Shortcut panel:

- LFA Type
- Relative Metric

9 If you enabled the Fast Reroute parameter in step 7, configure the parameters in the Fast Reroute panel:

- Backup Type
- Hop Limit
- Reserved Bandwidth (Mbps)
- Node Protect
- Propagate Administrative Groups

10 Configure the Make before Break parameter in the Make before Break panel.

11 Configure the parameters in the CSPF panel:

- Enable CSPF
- Enable TE Metric

12 Configure the parameters in the Signalling panel:

- Retry Timer (seconds)
- Retry Limit
- RSVP Reserve Style
- Include ADSPEC in RSVP
- Propagate Administrative Groups via Session Attribute Object

13 Configure the parameters in the Route Selection panel:

- Metric
- Least-Fill Path Selection

14 Configure the LDP over RSVP include parameter in the LDP Tunneling panel.

15 Configure the Enable Auto-Bind parameter in the Auto-Bind panel.

16 If you enabled the Auto Bandwidth parameter in step 7, configure the parameters in the Auto Bandwidth panel:

- Adjust Up Threshold (%)
- Adjust Down Threshold (%)
- Minimum Bandwidth (mbps)
- Monitor Bandwidth
- Sample Multiplier
- Overflow Limit
- Adjust Up Bandwidth (mbps)
- Adjust Down Bandwidth (mbps)
- Maximum Bandwidth (mbps)
- Adjust Multiplier
- Overflow Limit Threshold (%)
- Overflow Limit Bandwidth (mbps)
- FC BE Sampling Weight (%)
- FC AF Sampling Weight (%)
- FC H2 Sampling Weight (%)
- FC H1 Sampling Weight (%)
- FC L2 Sampling Weight (%)
- FC L1 Sampling Weight (%)
- FC EF Sampling Weight (%)
- FC NC Sampling Weight (%)

17 Click on the LSP-Path Bindings tab. A list of LSP paths is displayed.

18 Click on the Create button. The LSP-Path Binding step form opens and the Choose Path Type step is displayed. The Type parameter is set to secondary if a primary path exists.

19 Click on the Next button. The Choose MPLS Path step is displayed. Choose an MPLS path to associate with the LSP. You can also create an MPLS path by clicking on the Create MPLS Path button. See Procedure 25-4 for more information.

20 Click on the Next button. The Set Traffic Options step is displayed.

21 Configure the parameters:

- Reserved Bandwidth (Mbps)
- Hop Limit
- Inherit Value

22 Click on the Next button. The Set Initial States step is displayed.

23 Configure the Administrative State parameter.

24 Click on the Finish button. The LSP-Path Binding form closes and a dialog box appears.

25 Click on the OK button.

26 Click on the OK button. A dialog box appears.

27 Click on the Yes button. The Dynamic LSP (Edit) form closes.

28 Close the Manage Dynamic LSPs form.

Procedure 25-10 To create a dynamic LSP from a tunnel template

Before you can create an LSP from a tunnel template, you must create the tunnel template. You can use an existing LSP to create a tunnel template. See "XML API template script format" in the *5620 SAM Scripts and Templates Developer Guide* for more information about creating a tunnel template.

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form opens.

2 Click on the Create from Template button. A Create Dynamic LSP from Template form opens with a list of tunnel templates.

3 Choose a template from the list.

4 Click on the OK button. A Create Dynamic LSP from Template form opens.

5 Configure the parameters:

- Name
- Description
- ID
- Auto-Assign ID
- Preference
- Administrative State

6 Specify the source sites for the dynamic LSP.

i Click on the Select button beside the Source Site ID parameter. The Select Network Element form opens with a list of the available sites.

ii Choose a site from the list and click on the OK button. The Select a Network Element form closes and the Create Dynamic LSP from Template form displays the source site information.

iii Click on the Select button beside the Source IP Address parameter. The Select Network Element form opens with a list of the available sites.

iv Choose a site from the list and click on the Ok button. The Select a Network Element form closes and the Create Dynamic LSP from Template form displays the source IP address information.

7 Configure the Destination Site ID and the Destination IP Address parameters.

8 Click on the Accounting tab.

9 Click on the Select button beside the Accounting Policy parameter. A Select Policy form opens.

10 Choose a policy from the list.

11 Click on the OK button.

12 Configure the Collect Accounting Statistics and the Administrative State parameters.

13 Click on the Properties tab.

14 Configure the parameters:



Note — The number of parameters that can be configured depends on how the template was created. All of the parameters are configurable when the template is based on an object. A subset of the parameters can be configured when the template is based on an object class.

- Guarding Lsp
- Guarding Lsp
- Fast Reroute
- Hop Limit
- IGP Shortcut Enabled
- BGP RSVP LSP Transport Tunnel
- BGP Shortcut Enabled
- Diff-Serv Class Type
- Multi-Class Type Retry Limit
- Auto Bandwidth
- Propagate Administrative Groups
- LFA Type
- Relative Metric
- Backup Type
- Hop Limit
- Reserved Bandwidth (Mbps)
- Node Protect
- Retry Timer (seconds)
- RSVP Reserve Style
- Retry Limit
- Include ADSPEC in RSVP
- Make before Break
- Enable CSPF
- Enable TE Metric
- Metric
- Least-Fill Path Selection
- Groups Included
- Groups Excluded (bitmap)
- Persistent
- Permit Merge
- Record Actual Route
- Record Label
- Committed Rate
- Peak Rate
- Setup Priority
- Hold Priority
- Backup Setup Priority
- Backup Hold Priority
- LDP over RSVP include
- Enable Auto-Bind

15 Click on the OK button. The Create Dynamic LSP from Template form closes.

16 When the Show Created Object parameter is enabled on the template, the Dynamic LSP (Edit) form opens. Close the Dynamic LSP (Edit) form.

17 Close the Manage Dynamic LSPs form.

Procedure 25-11 To list dynamic LSPs

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form opens.

2 Configure the filter criteria. A list of dynamic LSPs is displayed.

3 Choose an LSP and click on the Properties button. The Dynamic LSP (Edit) form opens.

4 To view LSP path information:

i Click on the LSP Paths tab.

ii Double-click on an LSP path.

iii Review the state information.

The LSP path information includes whether the bypass tunnel for the LSP is active, or whether the LSP is in a fast reroute state.

Procedure 25-12 To run an OAM validation test for a dynamic LSP

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form opens.

2 Configure the filter criteria. A list of dynamic LSPs is displayed.

3 Choose an LSP and click on the Properties button. The Dynamic LSP (Edit) form opens.

4 Click the One Time Validation button.

5 Refer to Procedure 77-9 for more information on using the One Time Validation function and reviewing the test results.

Procedure 25-13 To create a Point-to-Multipoint LSP

1 Choose Manage→MPLS→Point-to-Multipoint LSPs from the 5620 SAM main menu. The Manage Point-to-Multipoint LSPs form opens.

2 Click on the Create button. The P2MP LSP (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Name
- ID
- Auto-Assign ID
- P2MPId
- Administrative
- System ID (Loopback IP Address)
- IP Address

When you configure the System ID (Loopback IP Address) parameter, the Management IP Address and Site Name parameters are automatically populated with the values associated with that NE. The IP Address parameter is also automatically populated, however, you can specify a new value for the parameter, if required.

4 Click on the Properties tab.

5 Configure the parameters in the Traffic Engineering and Protection panel:

- Fast Reroute
- Hop Limit

6 Configure the parameters in the Fast Reroute panel:

- Backup Type
- Hop Limit
- Reserved Bandwidth (Mbps)
- Node Protect
- Propagate Administrative Groups

The Node Protect parameter is only configurable when the Reserved Bandwidth (Mbps) parameter is set to a value greater than 0.

7 Configure the Make before Break parameter.

8 Configure the parameters in the CSPF panel:

- Enable CSPF
- Enable TE Metric

9 Configure the parameters in the Signalling panel:

- Retry Timer (seconds)
- Retry Limit
- RSVP Reserve Style
- Include ADSPEC in RSVP
- Propagate Administrative Groups via Session Attribute Object

10 Click on the P2MP Primary Instance tab.

11 Click the Create button. The P2MP Instance (Create) form opens with the General tab displayed.

12 Configure the parameters:

- Name
- ID
- Auto-Assign ID
- Administrative

13 Click on the Properties tab.

14 Configure the parameters in the Traffic Engineering Properties panel:

- Reserved Bandwidth (Mbps)
- Hop Limit
- Inherit Value
- Record Actual Path
- Record Label

When you enable the Inherit Value parameter, the Hop Limit parameter for the P2MP Instance is set to the same value as you configured for the parent P2MP LSP.

15 Configure the parameters in the Make Before Break panel:

- Make before Break
- Inherit Value
- Resignal

When you enable the Inherit Value parameter, the Make before Break parameter for the P2MP instance is set to the same value as you configured for the parent P2MP LSP.

16 Configure the parameters in the Administrative Groups panel:

- Inherit Value (for Groups Included)
- Inherit Value (for Groups Excluded)

When you enable the Inherit Value parameters, the Included and/or Excluded Groups for the P2MP instance are set to the same values you configure for the parent P2MP LSP. If you do not enable the Inherit Value parameters, you can configure the Included Groups and Excluded Groups for the P2MP Instance independently from the parent P2MP LSP. (See step 21.)

17 Click on the S2L Paths tab.

18 Click the Create button. The S2L Path (Create) form opens with the General tab displayed. Each S2L path object represents a root-to-leaf (S2L) sub-LSP path for the primary instance of the P2MP LSP.

19 Configure the parameters:

- Name
- ID
- Destination Site ID
- Administrative

20 Repeat steps 18 and 19 to configure another S2L path, if required.

21 Click on the Administrative Groups tab.

22 Assign one or more MPLS administrative groups to the P2MP Instance.

i Choose the required Included Groups in the Unassigned list.

ii Click on the right arrow button. The groups are assigned to the Point-to-Multipoint LSP and moved to the Assigned list.

iii Select the required Excluded Groups in the Unassigned list.

iv Click on the right arrow button. The groups are assigned to the Point-to-Multipoint LSP and moved to the Assigned list.

After you assign the Included and Excluded Groups, the total value of the groups is displayed in a bit mask format by the Groups Included and Groups Excluded indicators on the P2MP Instance Properties tab.

23 Click on the OK button. The P2MP Instance (Create) form closes.

24 Click on the S2L Paths tab in the main P2MP LSP (Create) form.

25 Click on the Search button to populate the table. The S2L Paths you configured in step 18 appears. You can choose an entry from the list and click on Properties to edit it, if required.

26 Click on the Administrative Groups tab in the main P2MP LSP (Create) form.

27 Assign one or more MPLS administrative groups to the P2MP LSP.

i Select the required Included Groups in the Unassigned list.

ii Click on the right arrow button. The groups are assigned to the Point-to-Multipoint LSP and move to the Assigned list.

iii Select the required Excluded Groups in the Unassigned list.

iv Click on the right arrow button. The groups are assigned to the Point-to-Multipoint LSP and move to the Assigned list.

After you assign the Included and Excluded Groups, the total value of the groups is displayed in a bit mask format by the Groups Included (bitmap) and Groups Excluded (bitmap) indicators on the P2MP LSP Properties tab.

28 Click OK to close the P2MP LSP (Create) form.

29 Close the Manage Point-to-Multipoint LSPs form.

30 To complete the configuration of the Point-to-Multipoint LSP, you must:

a Configure the required PIM tunnel interfaces. See Procedure 22-1.

b Configure tunnel interfaces on the required IGMP routing instance. See Procedure 23-46.

c Configure tunnel interfaces on the required multicast info policy. See Procedure 45-4.

31 After you complete the configuration of the Point-to-Multipoint LSP, you can reopen the P2MP LSP form to create, configure and run OAM diagnostics, if required.

i Click on the Tests tab. The Test Suite, P2MP Ping, and P2MP Trace tabs are displayed.

ii Create or search for the test suite or particular type of test you want to run from the tab pages. Click on either the Create or Search buttons as required.

iii Click the Execute button to run a selected test.

See chapters 32 and 77 for more information about how to configure OAM diagnostics.

Procedure 25-14 To create a Manual Bypass LSP

1 Choose Manage→MPLS→Manual Bypass LSPs from the 5620 SAM main menu. The Manage Manual Bypass LSPs form appears.

2 Click on the Create button. The Create Bypass-only LSP form opens with the Identification step displayed.

3 Configure the parameters:

- Name
- Description
- ID
- Auto-Assign ID

4 Click on the Next button. The Define Source and Destination Sites step is displayed.

5 Specify the source and destination sites for the manual bypass LSP.



Note — You can also manually specify an IP address for each parameter in this step.

i Click on the Source Site ID parameter Select button. The Select a Network Element - Create Bypass-only LSP form opens with a list of the available sites.

ii Choose a site and click on the OK button. The Select a Network Element - Create Bypass-only LSP form closes and the Create Bypass-only LSP form displays the source site information, which includes the Source IP Address parameter value. This parameter is automatically populated with the system IP address of the site.

iii Click on the Destination Site ID parameter Select button. The Select a Network Element - Create Bypass-only LSP form opens with a list of the available sites.

iv Choose a site and click on the OK button. The Select a Network Element - Create Bypass-only LSP form closes and the Create Bypass-only LSP form displays the destination site information. The displayed destination interface is the system interface because an LSP can terminate only on a system interface.

6 Click on the Next button. The Auto Select Hop-Less MPLS Path form opens.

7 Configure the Auto Select Hop-Less Path parameter.

8 If the Auto Select Hop-less Path parameter in step 7 is enabled, go to step 10.

9 Click on the Next button. The LSP-Path Binding opens, with the Choose MPLS Path step displayed.

i Choose an MPLS path to associate with the LSP. You can also create an MPLS path by clicking on the Create MPLS Path button. See Procedure 25-4.

ii Click on the Next button. The Set Traffic Options step is displayed.

iii Configure the parameters:

- Hop Limit
- Inherit Value
- Record Actual Path

iv Click on the Next button. The Set Initial States step is displayed.

v Configure the Administrative parameter.

vi Click on the Finish button. The LSP-Path Binding form closes and a dialog box appears.

vii Click on the OK button. The Create Bypass-only LSP form reappears.

10 Click on the Next button. The Properties step is displayed.

11 Configure the Hop Limit parameter in the Traffic Engineering And Protection panel.

12 Configure the Make before Break parameter in the Make before Break panel.

13 In the CSPF panel, configure the parameters:

- Enable CSPF
- TE Metric

14 Configure the parameters in the Signalling panel:

- Retry Timer (seconds)
- Retry Limit
- RSVP Reserve Style
- Include ADSPEC in RSVP
- Propagate Administrative Group via Session Attribute Object

15 Configure the parameters in the Inter Area/Level Traffic Engineering panel:

- Exclude Node in ERO
- Exclude Node IP Address

16 Click on the Next button. The Admin Groups step is displayed.

17 Assign one or more included MPLS administrative groups to the bypass-only LSP.

i Choose the required MPLS administrative groups in the Included Groups - Unassigned list.

ii Click on the right arrow button. The groups are assigned to the bypass-only LSP and move to the Assigned list.



Note — When you assign included administrative groups to an MPLS interface, the assigned groups are displayed in bit mask form by the Groups Included (bitmask) indicator on the General tab.

18 Assign one or more excluded MPLS administrative groups to the bypass-only LSP, if required.

i Choose the required MPLS administrative groups in the Excluded Groups - Unassigned list.

ii Click on the right arrow button. The groups are assigned to the bypass-only LSP and move to the Assigned list.



Note — When you assign excluded administrative groups to an MPLS interface, the assigned groups are displayed in bit mask form by the Groups Excluded (bitmask) indicator on the General tab.

19 Click on the Next button. The Set Initial State step is displayed.

20 Configure the Administrative parameter.

21 Click on the Finish button. The 5620 SAM prompts you to view the bypass-only LSP.

22 Enable the View the newly created Bypass Only Lsp parameter to view the bypass-only LSP configuration after closing the form, if required.

23 Click on the Close button. The Create Bypass-only LSP form closes.

24 If the View the newly created Bypass Only Lsp parameter in step 22 is enabled, the Bypass-only LSP (Edit) form opens with the newly created bypass-only LSP configuration displayed.

i View the configuration, if required.

ii Close the Bypass-only LSP (Edit) form.

25 Close the Manage Manual Bypass LSPs form.

Procedure 25-15 To configure a Manual Bypass LSP

1 Choose Manage→MPLS→Manual Bypass LSPs from the 5620 SAM main menu. The Manage Manual Bypass LSPs form opens.

2 Configure the filter criteria and click on the Search button. A list of bypass-only LSPs is displayed.

3 Choose an LSP and click on the Properties button. The Bypass-only LSP (Edit) form opens with the General tab displayed.

4 Configure the Description parameter in the Identity panel.

5 Configure the Administrative parameter in the States panel.

6 Click on the Properties tab.

7 Configure the Hop Limit parameter in the Traffic Engineering and Protection panel.

8 Configure the Make before Break parameter in the Make before Break panel.

9 Configure the parameters in the CSPF panel:

- Enable CSPF
- Enable TE Metric

10 Configure the parameters in the Signalling panel:

- Retry Timer (seconds)
- Retry Limit
- RSVP Reserve Style
- Include ADSPEC in RSVP
- Propagate Administrative Groups via Session Attribute Object

11 Configure the parameters in the Inter Area/Level Traffic Engineering panel:

- Exclude Node In ERO
- Exclude Node IP Address

12 Click on the OK button. A dialog box appears.

13 Click on the Yes button. The Bypass-only LSP (Edit) form closes.

14 Close the Manage Manual Bypass LSPs form.

Procedure 25-16 To configure an LSP path

The following procedure applies to Dynamic LSPs and Manual Bypass LSPs, unless otherwise noted. Dynamic LSPs are used to demonstrate the steps.

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form opens.

2 Configure the filter criteria and click on the Search button. A list of dynamic LSPs is displayed.

3 Choose a dynamic LSP from the list.

4 Click the on Properties button. The Dynamic LSP (Edit) form opens with the General tab displayed.

5 Click on the LSP-Path Bindings tab. A list of LSP paths is displayed.

6 If you are accessing this form to update the MPLS path for a Dynamic LSP, then go to step 14. Otherwise, go to step 7.

7 Choose an LSP-Path Binding from the list and click on the Properties button. The LSP-Path Binding (Edit) form opens with the General tab displayed.

8 Configure the Administrative parameter in the States panel.

9 Configure the parameters in the Transport Properties panel:

- Setup Priority
- Hold Priority

10 Configure the parameters in the Traffic Engineering Properties panel:

- Reserved Bandwidth (Mbps)
- Hop Limit
- Record Actual Path
- Record Label
- Diff-Serv Class Type
- Diff-Serv Backup Class Type

The Diff-Serv Backup Class Type parameter is only applicable to Dynamic LSPs.

11 Configure the parameters in the Make before Break panel:

- Make before Break
- Inherit Value
- Resignal

12 Configure the parameters in the Administrative Groups panel:

- Groups Included
- Inherit Value
- Groups Excluded (bitmap)
- Inherit Value

13 Replace the existing MPLS path for a primary or secondary LSP with another MPLS path, if required, by proceeding as follows:



Note — You can update the existing MPLS path only for a primary or secondary LSP path that has the Make before Break parameter enabled. The MPLS path you want to use must already exist on the NE, and must not be used by any other LSP paths under the parent LSP.

i Click on the Update MPLS Path button. If the Update MPLS Path button is not visible, click on the More Actions button and choose Update MPLS Path. The Choose MPLS Path form opens and displays the eligible MPLS paths.

ii Choose the required MPLS path from the list.

iii Click on the OK button. The Choose MPLS Path form closes and the LSP-Path Binding (Edit) form is refreshed with the parameters related to the updated MPLS path selection.

iv Click on the OK button. The The LSP-Path Binding (Edit) form closes and the LSP-Path Binding list is refreshed with the updated MPLS path selected.

v Go to step 18.

14 Choose the MPLS path from the list that you want to use to replace the existing path. See step 13 for restrictions.

15 Click on the Update MPLS Path button. If the Update MPLS Path button is not visible, click on the More Actions button and choose Update MPLS Path. The Choose MPLS Path form opens and displays the eligible MPLS paths.

16 Choose the required MPLS path from the list.

17 Click on the OK button. The Choose MPLS Path form closes and the LSP-Path Binding list is refreshed with the updated MPLS path selected.

18 Click the Set as Secondary or Set as Standby buttons for a selected LSP-Path Binding to change its Type to one of these choices, if required.

19 Click the Switch Standby to Standby button for a selected LSP-Path Binding if you need to switch from the current active standby LSP path to another standby LSP path. This applies only to dynamic LSPs. The button choices include:

- Switch: This option allows you to switch manually from an active standby path to another inactive standby path. You can do this as often as required, without having to select Clear first.
- Force Switch: This option is essentially the same as the Switch option, but you cannot switch back unless you first press Clear to remove the Force Switch flag.
- Clear: This option is used to clear the Force Switch flag.

20 Click on the Administrative Groups tab.

21 Assign an MPLS administrative group to the dynamic LSP.

i Choose an MPLS administrative group in the Unassigned list.

ii Click on the right arrow button. The group is assigned to the dynamic LSP and moves to the Assigned list.

After you assign administrative groups to an MPLS interface, the total value of the assigned groups is displayed in a bit mask format by the Groups Included (bitmask) indicator on the General tab.

22 Click on the General Tab and in the Shared Risk Link Group panel, configure the Enable SRLG for FRR or Enable SRLG parameter, if available and required.

23 Click on the Tests tab to configure OAM diagnostics for the LSP path, if required. The supported test type tabs appear. See chapter 32 for more information about how to configure OAM diagnostics.

24 View a list of hops, if required.

i Click on the following tabs to list the path hops, if required:

- Provisioned Path
- Actual Path
- CSPF Path

ii Click on the Topology View button to view the topology map for the path, if required. See chapter 6 for information about using topology maps.

25 Click on the OK button. The LSP-Path Binding (Edit) form closes.

26 Click on the OK button. The Dynamic LSP (Edit) form closes.

Procedure 25-17 To create an LSP path using a tunnel template

Before you can create an LSP path from a tunnel template, you must create the tunnel template. You can use an existing LSP path to create a tunnel template. See "XML API template script format" in the *5620 SAM Scripts and Templates Developer Guide* for more information about creating a tunnel template.

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form opens.

2 Click on the Create from Template button. A Create Dynamic LSP from Template form opens with a list of previously created templates.

3 Choose a LSP template from the list. The template must be one where you associated a child LSP Path template to the parent LSP template.

4 Click on the OK button. A Create Dynamic LSP from Template form opens. See Procedure 25-10 for information about creating a dynamic LSP from a template.

5 Click on the OK button. Perform one of the following:

   a If the Show Created Object parameter is enabled on the template, the Dynamic LSP (Edit) form opens. Go to step 6.

   b Open the Dynamic LSPs (Edit) form.

      i Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form opens.

      ii Choose the dynamic LSP that you created in step 4.

      iii Click on the Properties button. The Dynamic LSP (Edit) form opens.

6 Click on the LSP-Path Bindings tab.

7 Click on the Create from Template button. A pop-up menu appears with an LSP path template.

8 Click on the template that you need to use for the LSP path.

9 Configure the parameters:

- Type
- Administrative
- Fast Reroute
- Backup Type
- Hop Limit
- Backup Setup Priority
- Backup Hold Priority
- Minimum Bandwidth (mbps)
- Committed Rate
- Peak Rate
- Setup Priority
- Hold Priority
- Reserved Bandwidth
- Hop Limit
- Record Actual Path
- Record Label
- Persistent
- Permit Merge
- IGP Shortcut Enabled
- Diff-Serv Class Type
- Diff-Serv Backup Class Type
- Main Class Type Retry Limit
- Make before Break
- Resignal
- Enable CSPF
- Rebuild Timer
- Groups Included
- Groups Excluded (bitmap)
- Groups Included
- Enable SRLG

10 Click on the Inheritance tab.

11 Configure the Overridden Properties parameter.

12 Click on the OK button. A dialog box appears.

13 Click on the OK button. The Create LSP Path From Template form closes.

14 Close the Manage Dynamic LSPs form.

Procedure 25-18 To configure an LSP Path optimization policy

1 Choose Manage→MPLS→LSP Path Optimization from the 5620 SAM main menu. The Manage LSP Path Optimization form opens.

2 Choose LSP Path Optimization Policy (Path/Routing Management: MPLS) from the drop-down menu.

3 Click on the Create button. A drop-down menu appears.

4 Choose Create Optimization Policy. The LSP Path Optimization Policy (Create) form opens with the General tab displayed.

5 Configure the parameters:

- ID
- Auto-Assign ID
- Description

6 Click on the Candidate Definition tab to apply filters to define eligible LSP Paths for optimization. When no filters are applied, all eligible LSP Paths are listed in the Execution Candidates form.

7 To further limit the number LSP Paths that are listed in the Execution Candidate form, define rule-based groups and add only those NEs that contain the LSP Paths that you need include.

i Click on Select button beside the Filter Name parameter in the LSP Path Filter panel. A Select LSP Path Filter dialog box appears.

ii Apply a filter, or create and apply a filter and click on the Search button. A list of LSP Path filters is displayed.

iii Choose an LSP Path filter from the list.

iv Click on the OK button. The LSP Path Filter panel is refreshed with the selected LSP Path Filter.

v Click on the Select button beside the Filter Name parameter in the Dynamic LSP Filter panel.

vi Apply a filter, or create and apply a filter and click on the Search button. A list of dynamic LSP filters is displayed.

vii Choose a dynamic LSP filter from the list

viii Click on the OK button. The Dynamic LSP Filter panel is refreshed with the selected dynamic LSP filter.

ix Click on the Select button beside the Name parameter in the Rule-Based Group panel. A list of rule-based groups is displayed

x Choose a rule-based group from the list.

xi Click on the OK button. The Rule-Based Group panel is refreshed with the selected rule-based group.

8 Click on the Execution Rules tab. Configure the parameters:

- Sequencing Target
- Sequencing Order
- Pacing Interval (seconds)

9 Click on the Apply button. The form displays with schedule information.



Note 1 — The Schedule Optimization button does not appear during LSP path optimization policy creation. The LSP path optimization policy must be created first before a schedule can be applied. You must click on the Apply button.

Note 2 — After a schedule is applied to a LSP Optimization Policy, you cannot make changes to the schedule from the Optimization Scheduled Task form.

10 Click on the Schedule Optimization button. An Optimization Scheduled Task (Create) form opens.

11 Configure the parameters:

- Scheduled Task Name
- Scheduled Task Description
- Administrative State

12 Click on the Select button beside the ID parameter. A Select Schedule - Optimization Scheduled Task form opens.

13 Perform one of the following:

a Click on the Create button to create a schedule. A SAM Schedule Create form opens. See Procedure 7-1 for more information about how to create a schedule.

b Choose a previously created schedule.

14 Click on the OK button. The Optimization Scheduled Task form displays schedule and optimization information.

15 Click on the OK button. The Select Schedule - Optimization Scheduled Task form closes and the LSP Path Optimization Policy form reappears.

16 Click on the Execution Candidates tab.

17 Click on the Search button to display only the eligible LSP Paths that were filtered in step 7. If a filter was not applied, all eligible LSP Paths are listed.

18 Click on the Optimize button. To view the results of optimization, see Procedure 25-20.

19 Close the LSP Path Optimization Policy form.

Procedure 25-19 To terminate an LSP Path optimization policy that is in progress

1 Choose Manage→MPLS→LSP Path Optimization from the 5620 SAM main menu. The Manage LSP Path Optimization form opens.

2 Choose LSP Path Optimization Policy (Path/Routing Management: MPLS) from the drop-down menu.

3 Create a filter to search for optimization policies that are in progress. Click on the Search button. A list of LSP Path optimization policies that are in progress appears.

4 Choose a LSP Path optimization policy from the list.

5 Click on the Properties button. The LSP Path Optimization Policy (Edit) form opens with the General tab displayed.

6 Click on the Stop Current Optimization button. If the Stop Current Optimization button is not visible, click on the More Actions button and choose Stop Current Optimization. The Optimization parameter value changes from In Progress to Not In Progress.

7 Close the LSP Path Optimization Policy (Edit) form.

Procedure 25-20 To view LSP Path optimization policy results

Use the following procedure to view the re-signaling information as a result of the LSP Path optimization policy execution. See Procedure 25-18 for more information about how to configure a LSP Path optimization policy.

1 Choose Manage→MLPS→LSP Path Optimization from the 5620 SAM main menu. The Manage LSP Path Optimization form opens.

2 Choose LSP Path (Path/Routing Management MPLS) from the drop-down menu.

3 Click on the Search button. A list of LSP Paths appears.

4 Choose the LSP Path on which you executed a LSP optimization policy.

5 Click on the Properties button. An LSP-Path Binding (Edit) form opens.

6 View the parameters, as described in section 25.1.

- Resignal Eligible
- Last Performed Type
- Last Performed
- Last Performed State

7 Close the LSP-Path Binding form.

8 Close the Manage LSP Path Optimization form.

Procedure 25-21 To view detour and bypass path information

Perform this procedure to view information regarding detour and bypass tunnel paths and their protected LSPs. Detour and bypass paths are typically configured for fast-reroute-enabled LSPs on NEs for service protection against NE or link failure. The RSVP protocol is used to detect an NE or link loss.



Note 1 — This procedure applies to dynamic LSPs only.

Note 2 — Detours are employed in One-to-One backup configurations. A separate backup LSP is established for each LSP that is backed up.

Bypass Tunnels are employed in Many-to-One backup configurations in which a single backup LSP is used to back up multiple original LSPs.

Whether a path is a detour or bypass path is determined by the Backup Type parameter value specified during LSP creation. The Backup Type parameter can be set only when the Fast Reroute parameter for the LSP is set to true.

1 Navigate to a dynamic LSP that you want to examine. The path is Manage→MPLS→Dynamic LSPs.

2 Choose the required LSP and click on the Properties button. The Dynamic LSP (Edit) form opens.

3 Click on the RSVP Sessions tab. The detour or bypass originating, transiting, and terminating RSVP sessions associated with the LSP are listed. Type, site, next and previous hop, and other related information is available.



Note — The SRLG Disjoint FRR Properties and SRLG Not Strict FRR Properties indicators apply to primary LSP sessions only, and not to bypass LSP sessions.

4 Choose the desired RSVP session of type detour or bypass from the list and click on the Properties button. The Session (View) form opens.

5 To view the Protected LSPs for the specific bypass or detour:

- **i** Click on the Protected LSP Paths tab. All the protected LSPs for a specific bypass or detour tunnel are listed.
- **ii** Use the scroll bar at the bottom of the list frame to view the available information on the Protected LSPs.

6 To view the Detour or Bypass Tunnel Paths for the detour or bypass tunnel:

i Click on the Detour/Bypass Tunnel Path tab. Information regarding the detour or bypass paths is displayed. Sufficient information is provided to permit tracing a path from its originating site, through its transit hops, and to its termination site.

ii Use the scroll bar at the bottom of the list frame to view the available information on the paths, including ID, Type, and so on.

7 To view additional specific Detour or Bypass information, perform the following steps, as appropriate:

a For a selected detour session, click on the Detour tab. The Detour Session ID, Detour PLR ID, and Avoided Downstream Site ID are listed.

b For a selected bypass session, click on the Bypass Tunnel tab. The Bypass Tunnel's current State is displayed.



Note — For 5620 SAM to accurately gather the information about the detour and bypass tunnel path (and the LSPs protected by a detour or a bypass tunnel), 5620 SAM must be managing all routers participating the LSP fast reroute. This is required by 5620 SAM for all SR and 7705 SAR network elements along the primary path of a fast reroute-enabled LSP.

Procedure 25-22 To view exclude route object information

Perform this procedure to view the address of the NE to be avoided as signalled in the EXCLUDE_ROUTE object.



Note — This procedure applies to dynamic LSPs only.

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form opens.

2 Choose a dynamic LSP and click on the Properties button. The Dynamic LSP (Edit) form opens with the General tab displayed.

3 Click on the RSVP Sessions tab.

4 Choose the desired RSVP session from the list and click on the Properties button. The Session (View) form opens with the General tab displayed.

5 View the Exclude Node IP Address property. If no EXCLUDE_ROUTE object is signalled, the address is 0.0.0.0.

6 Close the Session (View) form.

7 Close the Dynamic LSP (Edit) form.

8 Close The Manage Dynamic LSPs form.

Procedure 25-23 To create an LSP template for MVPN

1 Choose Policies→MPLS→LSP Template MVPN from the 5620 SAM main menu. The LSP Template MVPN Policies form opens.

2 Perform one of the following:

a Configure the Policy scope parameter to Global.

b Configure the Policy scope parameter to Local.

i Configure the Local Node IP Address parameter, if required.

ii Click on the Select button and choose a device.

3 Click on the Create button. The LSP Template MVPN Policy (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Displayed Name
- Description

5 Click on the Properties tab.

6 Configure the parameters in the Traffic Engineering and Protection panel:

- Reserved Bandwidth (Mbps)
- Fast Reroute
- Hop Limit
- Record Actual Path
- Record Label

7 Configure the parameters in the Fast Reroute panel:

- Backup Type
- Hop Limit
- Propagate Administrative Groups

Note — The Fast Reroute panel parameters are configurable if the Fast Reroute parameter is set to true.

8 Configure the Make before Break parameter.

9 Configure the parameters in the CSPF panel:

- Enable CSPF
- Enable TE Metric

10 Configure the parameters in the Signalling panel:

- Retry Timer (seconds)
- Retry Limit
- Propagate Administrative Groups via Session Attribute Object

11 Click on the Administrative Groups tab.

12 Assign one or more MPLS administrative groups to the LSP template MVPN policy.

i Choose the required Included Groups in the Unassigned list.

ii Click on the right arrow button. The groups are assigned to the Point-to-Multipoint LSP and moved to the Assigned list.

iii Choose the required Excluded Groups in the Unassigned list.

iv Click on the right arrow button. The groups are assigned to the Point-to-Multipoint LSP and moved to the Assigned list.

After you assign the Included and Excluded Groups, the total value of the groups is displayed in a bit mask format by the Groups Included and Groups Excluded indicators on the LSP Template MVPN Policy Properties tab.

13 Click on the OK button. The LSP Template MVPN Policy, Global Policy (Create) form closes and the Manage Lsp Template for Mvpn form reappears with the LSP MVPN template displayed.

14 Choose the LSP MVPN template and click on the Properties button. The LSP Template MVPN Policy - Global Policy (Edit) form opens with the General tab displayed.

15 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when the policies are used by resources on the device.



Note 1 — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution, which also distributes the policy to existing local definitions. See chapter 42.

Note 2 — The MVPN LSP template cannot be used until you choose a default MPLS path and configure the Administrative parameter in the local policy definition after the global policy is distributed. After the changes are applied to the local policy, the policy can be switched back to Sync With Global mode and the local changes are saved.

16 Click on the Local Definitions tab.

17 Click on the Search button. A list of LSP MVPN templates is displayed.

18 Choose an LSP MVPN template from the list and click on the Properties button. The LSP Template MVPN Policy, Local Policy (Edit) form opens with the General tab displayed.

19 Click on the Switch Mode button to change the configuration mode to Local Edit Only.

20 Click on the Properties tab.

21 Click on the Select button to choose a default MPLS path. The Select Default MPLS Path - Lsp MVPN Template, Local Policy form opens with a list of default MPLS paths displayed.

22 Choose an MPLS path from the list and click on the OK button. The default MPLS path is displayed.

23 Click on the General tab.

24 Configure the Administrative parameter.

25 Click on the OK button. A dialog box appears.

26 Click on the OK button. The LSP Template MVPN Policy, Local Policy form closes.

Procedure 25-24 To view LSP templates for MVPN created using CLI

Perform this procedure to view read-only one-hop P2P LSP and mesh P2P LSP templates created using CLI.

You cannot modify the local or global definitions of these template types using the 5620 SAM. You cannot distribute these template types to other NEs using the 5620 SAM. See the specific device documentation for more information about how to create a one-hop P2P LSP or mesh P2P LSP template.

1 Choose Policies→MPLS→LSP Template MVPN from the 5620 SAM main menu. The LSP Template MVPN Policies form opens.

2 Perform one of the following:

- **a** Configure the Policy scope parameter to Global.
- **b** Configure the Policy scope parameter to Local.
  - **i** Configure the Local Node IP Address parameter, if required.
  - **ii** Click on the Select button and choose an NE.

3 Choose one of the following from the Type column drop-down menu.

- One-Hop P2P LSP
- Mesh P2P LSP

4 Click on the Search button. A list of LSP templates for MVPN is displayed.

5 Choose an LSP template and click on the Properties button. The LSP Template MVPN Policy - *template_type* (View) form opens with the General tab displayed.

6 Choose the LSP MVPN template and click on the Properties button. The LSP Template MVPN Policy - Global Policy (Edit) form opens with the General tab displayed.

7 Click on the tabs to view information about the LSP template.

8 Close the LSP Template MVPN Policy - *template_type* (View) form.

9 Close the LSP Template MVPN Policies form.

Procedure 25-25 To view LSPs created by one-hop P2P and mesh P2P templates

Dynamic LSPs are automatically created when you use CLI to create and distribute a one-hop P2P or mesh P2P LSP template, and then associate the LSP template with an auto-LSP. Perform the following procedure to view the LSPs that are automatically created by one-hop P2P and mesh P2P templates.



Note — The dynamically-created LSPs cannot be associated with SDPs, and are not listed when you are creating an SDP.

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form opens.

2 Choose one of the following from the Type column drop-down menu.

- One-Hop Point-To-Point
- Mesh Point-To-Point

3 Click on the Search button. A list of dynamic LSPs is displayed.

4 Choose an LSP and click on the Properties button. The properties form for the object appears.

5 View the information on the various tabs, as required.

6 Close the object properties form.

7 Close the Manage Dynamic LSPs form.

Procedure 25-26 To list and view MPLS objects

1 Choose Manage→MPLS→MPLS Objects from the 5620 SAM main menu. The Manage MPLS Objects form opens.

2 Choose an MPLS object type and click on the Search button. A list of MPLS objects is displayed.

3 Choose an object and click on the Properties button. The properties form for the object appears.

4 View the information on the various tabs, as required.

5 Close the object properties form.

6 Close the Manage MPLS Objects form.

26 — MPLS-TP

26.1 MPLS-TP overview *26-2*

26.2 Simplified provisioning *26-3*

26.3 Workflow to configure MPLS-TP *26-3*

26.4 MPLS-TP procedures *26-4*

26.1 MPLS-TP overview

MPLS-TP is a set of MPLS protocol functions that enables the use of MPLS in transport networks and applications. MPLS-TP provides in-band proactive OAM and protection mechanisms that do not rely on a control plane, such as RSVP-TE, to operate. MPLS-TP enables MPLS to be deployed in a statically configured transport network without the need for a dynamic control plane.

The 7450 ESS, 7750 SR, and 7950 XRS have two primary roles in an MPLS-TP network:

- as a gateway PE between IP/MPLS and MPLS-TP domains
- as an LSR or LER for MPLS-TP LSPs

The 5620 SAM can configure LSR NEs even when LERs are not configured, or when the LERs or LSRs are not a 7450 ESS, 7750 SR, or 7950 XRS. See the specific NE documentation for more information about MPLS-TP.

The 5620 SAM provides simple provisioning for MPLS-TP management in a transport network. MPLS-TP relies on static configuration, rather than a control plane, to ensure end-to-end path configuration and consistency. The 5620 SAM support of MPLS-TP includes:

- bidirectional co-routed MPLS-TP LSPs and PWs
- MPLS-TP identifiers for NEs, LSPs, and PWs
- linear protection for MPLS-TP LSPs with working and protection paths for each LSP
- OAM and protection with both IP and non-IP encapsulation
- proactive CC/V for MPLS-TP LSPs using BFD
- on-demand CV for MPLS-TP LSPs and PWs using LSP ping and trace and VCCV ping and trace diagnostics
- static PW status signaling, with support for PW redundancy, MC-LAG, MC-APS, BGP multi-homing and active and standby dual-homing into IES, VPRN, or VPLS

Proactive OAM

A proactive continuity check detects a loss of continuity defect between two MEPs in a MEG. Proactive connectivity verification detects an unexpected connectivity defect between two MEPs, and unexpected connectivity within the MEG with an unexpected MEP. The 5620 SAM implements both tests with a proactive OAM template.

Proactive OAM templates are based on BFD. BFD packets are sent using configurable timers. Continuity check packets contain a BFD control packet, while connectivity verification packets also include an identifier for the source MEP. The destination MEP can detect a connectivity defect if it is receiving packets from an incorrect peer MEP. When a defect is detected, the 5620 SAM generates an alarm.

26.2 Simplified provisioning

The 5620 SAM significantly simplifies the provisioning process of bidirectional MPLS-TP LSPs, where using CLI can be cumbersome and prone to error. Using the 5620 SAM, all of the components of an end-to-end bidirectional MPLS-TP LSP are automatically configured. Using CLI, all of the components of a bidirectional MPLS-TP LSP, including interfaces and labels, must be configured. The 5620 SAM automatically creates opposite interfaces based on the physical links between NEs, and assigns in and out labels across all of the interfaces. However, if a physical link does not exist between NEs, the 5620 SAM cannot auto-create the interfaces. The 5620 SAM prompts you to manually create the interfaces.

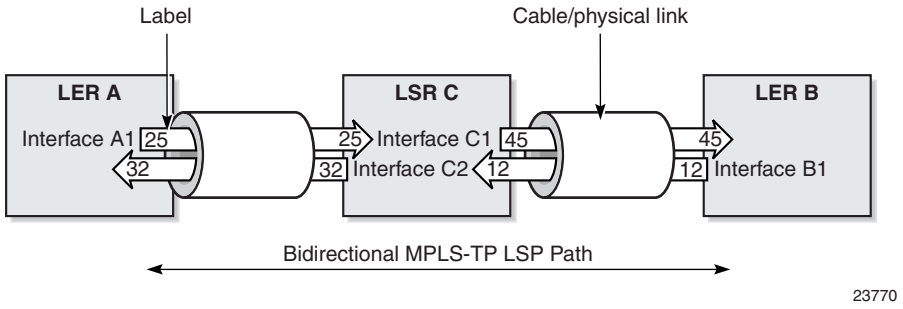
Consider the following when you create a bidirectional MPLS-TP LSP using 5620 SAM simplified provisioning:

- the NEs must be 5620 SAM-managed
- MPLS-TP tunnels that are created on the NEs using CLI are discovered by the 5620 SAM

Note — The 5620 SAM does not create the bidirectional MPLS-TP LSP when all of the MPLS-TP LSP endpoints (LERs) are not managed by the 5620 SAM. However, cross-connections (on LSRs) appear in the 5620 SAM database if the LSRs are managed.

In the example in Figure 26-1, you configure the LER A and LER B using the 5620 SAM. For the bidirectional MPLS-TP LSP path, you identify the hops by specifying the interfaces. In this example, the interfaces are A1 on LER A and C1 on LSR C. Since MPLS-TP is co-routed, the other interfaces (B1 and C2) are determined by the 5620 SAM based on the link between the two NEs. The 5620 SAM automatically chooses all of the labels, in both directions, based on the available labels on the two adjacent NEs. The 5620 SAM also creates the LSR C object. You must configure proactive OAM on LER NEs.

Figure 26-1 Sample bidirectional MPLS-TP LSP



26.3 Workflow to configure MPLS-TP

1 Enable MPLS-TP on the routing instances of all NEs that are to participate in the MPLS-TP network. See Procedure 26-1.

2 Create or configure an MPLS-TP instance. See Procedure 26-2.

3 Create a BFD template policy, if required. See Procedure 26-3.

4 Configure proactive OAM templates and protection templates, if required. See Procedures 26-4 and 26-5.

5 Perform one of the following, as required:

a Create a mesh of MPLS-TP LSPs. See Procedure 26-6. Create an MPLS-TP LSR cross-connect path. See Procedure 26-7.

b Create a bidirectional MPLS-TP LSP using simplified provisioning. See Procedure 26-8.

6 Create a service tunnel, if required, and enable MPLS-TP. See Procedure 27-1.

7 Create a spoke SDP binding using an MPLS-TP service tunnel, if required, on an Apipe, Epipe, Cpipe, VPLS, VPRN, IES, or mirror service. See Procedures 67-4, 67-10, 67-23, 68-44, 71-57, 70-8, and 69-3.

8 Configure static MPLS-TP pseudowire, if required, on a VPLS, VPRN, IES, Epipe, Cpipe or Apipe VLL, or on a mirror service. Ensure that the Control Word parameter for pseudowire OAM is set to Preferred. See Procedures 67-5, 67-11, 67-24, 68-45, 69-4, 70-9, and 71-58.

26.4 MPLS-TP procedures

Use the following 5620 SAM procedures to manage MPLS-TP.

Procedure 26-1 To enable MPLS-TP on a routing instance

1 Choose Routing→NE→Routing Instance from the 5620 SAM navigation tree view selector.

2 Right-click on the routing instance and choose Properties from the contextual menu. The Routing Instance (Edit) form opens with the General tab displayed.

3 Click on the Protocols tab.

4 Enable the MPLS Enabled parameter.

5 Enable the MPLS-TP Enabled parameter.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The Routing Instance (Edit) form closes. The 5620 SAM creates an MPLS-TP site and displays the site below the routing instance in the routing navigation tree.

Procedure 26-2 To configure an MPLS-TP instance

Ensure that you enable MPLS-TP on all of the NEs that are participating in the MPLS-TP network, as described in Procedure 26-1.

1 Navigate to an MPLS-TP instance by choosing Routing→NE→Routing Instance→MPLS-TP from the 5620 SAM navigation tree.

2 Right-click on the MPLS-TP instance, and choose Properties from the contextual menu. The MPLS-TP, Routing Instance (Edit) form opens with the General tab displayed.

3 Configure the parameters in the MPLS-TP General Configurations panel:

- Global ID
- Node ID
- TP-LSP ID Minimum
- TP-LSP ID Maximum

The Global ID and Node ID parameters are identifiers of an MPLS-TP site on the NE. The TP-LSP ID Minimum and TP-LSP ID Maximum parameters reserve a range of IDs that you use for MPLS-TP LSPs.

4 Configure the Administrative State parameter in the States panel.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The MPLS-TP, Routing Instance (Edit) form closes.

Procedure 26-3 To create an MPLS-TP BFD template policy

Perform this procedure to create a BFD template policy that you can assign to a proactive OAM policy in Procedure 26-4.

1 Choose Policies→MPLS→MPLS-TP BFD Templates from the 5620 SAM main menu. The Manage MPLS-TP BFD Templates form opens.

2 Click on the Create button. The BFD Template, Global Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Transmit Timer (milliseconds)
- Receive Timer (milliseconds)
- Multiplier
- Echo Receive Interval (milliseconds)
- Template Type

4 Click on the Apply button. The BFD Template (Edit) form refreshes with additional tabs.

5 Release and distribute the policy. See Procedure 42-1.

6 Close the BFD Template, Global Policy (Edit) form.

7 Close the Manage MPLS-TP BFD Templates form.

Procedure 26-4 To configure a proactive OAM template on an MPLS-TP instance

1 Choose Routing→NE→Routing Instance→MPLS-TP from the 5620 SAM navigation tree.

2 Right-click on the MPLS-TP instance in the navigation tree, and choose Properties from the contextual menu. The MPLS-TP, Routing Instance (Edit) form opens with the General tab displayed.

3 Click on the Proactive OAM Template tab.

4 Click on the Create button. The Proactive OAM Template, Routing Instance (Create) form opens with the General tab displayed.

5 Configure the parameters:

- Displayed Name
- Hold Time Down (centiseconds)
- Hold Time Up (centiseconds)

6 Click on the Select button in the BFD Template panel. The Select BFD Template - Proactive OAM Template list form opens.

7 Specify a search filter, if required, and click on the Search button. A list of configured BFD templates appears. See Procedure 26-3 for information about how to create a BFD template policy.

8 Choose a BFD template and click on the OK button. The Select BFD Template - Proactive OAM Template list form closes and the Proactive OAM Template (Create) form refreshes with the BFD template information.

9 Click on the OK button. The Proactive OAM Template (Create) form closes and a dialog box appears.

10 Click on the OK button.

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The MPLS-TP, Routing Instance (Edit) form closes.

Procedure 26-5 To configure a protection template on an MPLS-TP instance

1 Choose Routing→NE→Routing Instance→MPLS-TP from the 5620 SAM navigation tree.

2 Right-click on the MPLS-TP instance in the navigation tree, and choose Properties from the contextual menu. The MPLS-TP, Routing Instance (Edit) form opens with the General tab displayed.

3 Click on the Protection Template tab.

4 Click on the Create button. The Protection Template, Routing Instance (Create) form opens with the General tab displayed.

5 Configure the parameters:

- Displayed Name
- Revertive
- Wait To Restore (seconds)
- Rapid Protection Switch Coordination (milliseconds)
- Slow Protection Switch Coordination (milliseconds)

6 Click on the OK button. The Protection Template, Routing Instance (Create) form closes and a dialog box appears.

7 Click on the OK button.

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button. The MPLS-TP, Routing Instance (Edit) form closes.

Procedure 26-6 To create an MPLS-TP LSP

1 Choose Manage→MPLS→MPLS-TP LSPs from the 5620 SAM main menu. The Manage MPLS-TP LSPs form opens.

2 Click on the Create button and choose Create LER TP-LSP. The LER TP-LSP (Create) form opens with the General tab displayed.

3 Configure the parameters in the Identity panel:

- Name
- TP-LSP ID
- Auto-Assign ID

The TP-LSP ID must be in the range of the TP-LSP ID Minimum and TP-LSP ID Maximum parameters that you specified in step 3 of Procedure 26-2.

4 Click on the Select button in the Source Site panel. The Select Source Site - LER TP-LSP list form opens.

5 Choose a source site and click on the OK button. The Select Source Site - LER TP-LSP list form closes.

6 Configure the parameters in the Destination panel:

- Destination Tunnel Number
- Destination Node ID
- Destination Global ID

7 Click on the TP-LSP Path tab.

8 Click on the Create button. The MPLS-TP LSP Path (Create) form opens with the General tab displayed.



Note — You can create one working path and one protecting path.

9 Configure a working path:

i Set the Path Type parameter to Working in the Identity panel.

ii Configure the Administrative parameter in the States panel.

iii Configure the parameters:

- LSP Path Number
- Ingress Label
- Egress Label

iv Click on the Select button in the Out Link panel. The Select Out Link - TP-LSP Path list form opens.

v Click on the Search button. A list of configured routing interfaces (numbered or MPLS-TP unnumbered) appears.

vi Choose a site and click on the OK button. The Select Out Link - TP-LSP Path list form closes.

vii If you choose a numbered outlink interface, configure the Next Hop parameter.

viii Go to step 11.

10 Configure a protecting path:

i Set the Path Type parameter to Protecting in the Identity panel.

ii Configure the parameters:

- LSP Path Number
- Ingress Label
- Egress Label

iii Configure the Administrative parameter in the States panel.

iv Click on the Select button beside the Interface Name parameter in the Out Link panel. The Select Out Link - MPLS-TP LSP Path list form opens.

v Click on the Search button. A list of configured routing interfaces (numbered or MPLS-TP unnumbered) appears.

vi Choose an interface and click on the OK button. The Select Out Link - MPLS-TP LSP Path list form closes.

vii If you choose a numbered outlink interface, configure the Next Hop parameter.

11 Configure a path MEP.

i Click on the Path MEP tab.

ii Click on the Create button. The Path MEP (Create) form opens with the General tab displayed.

iii Click on the Select button beside the Proactive OAM Template parameter. The Select Proactive OAM Template - Path MEP list form opens with a list of configured proactive OAM templates.

iv Choose a proactive OAM template and click on the OK button. The Select Proactive OAM Template - Path MEP list form closes.

v If you are configuring a protecting MEP, click on the Select button beside the Protection Template parameter. Otherwise, go to step vii. The Select Protection Template - Path MEP list form opens with a list of configured protection templates.

vi Choose a protection template and click on the OK button. The Select Protection Template - Path MEP list form closes.

vii Configure the parameters:

- Administrative State
- BFD Enabled

viii Click on the OK button. The Path MEP (Create) form closes and a dialog box appears.

ix Click on the OK button.

12 Go to step 10 to create a protecting path. Otherwise, go to step 13.

13 Click on the OK button. The TP-LSP Path (Create) form closes and a dialog box appears.

14 Click on the OK button.

15 Click on the OK button. The LER TP-LSP Path (Create) form closes and a dialog box appears.

16 Click on the OK button.

17 Close the Manage MPLS-TP LSPs form.

Procedure 26-7 To create an MPLS-TP LSR cross-connect path

1 Choose Manage→MPLS→MPLS-TP LSPs from the 5620 SAM main menu. The Manage MPLS-TP LSPs form opens.

2 Click on the Create button and choose Create LSR Path. The LSR Path (Create) form opens with the General tab displayed.

3 Configure the Display Name parameter in the Identity panel.

4 Click on the Select button beside the Site ID parameter to choose the site that is used as the cross-connect. The Select Site - LSR Path list form opens.

5 Choose a site and click on the OK button. The Select Site - LSR Path list form closes.

6 Configure the Administrative parameter in the States panel.

7 Configure the parameters:

- Forward Path Enabled
- Reverse Path Enabled

8 If you enabled the Forward Path Enabled parameter in step 7, perform the following. Otherwise, go to step 10.

i Configure the parameters:

- Forward Ingress Label
- Forward Egress Label

ii Click on the Select button in the Forward Out Link panel. The Select Forward Out Link - LSR Path list form opens.

iii Click on the Search button. A list of configured routing interfaces (numbered or MPLS-TP unnumbered) appears.

iv Choose a site and click on the OK button. The Select Forward Out Link - LSR Path list form closes.

v If you choose a numbered outlink interface, configure the Forward Next Hop parameter.

9 If you enabled the Reverse Path Enabled parameter in step 7, perform the following. Otherwise, go to step 10.

i Configure the parameters:

- Reverse Ingress Label
- Reverse Egress Label

ii Click on the Select button in the Reverse Out Link panel. The Select Reverse Out Link - LSR Path list form opens.

iii Click on the Search button. A list of configured routing interfaces (numbered or MPLS-TP unnumbered) appears.

iv Choose a site and click on the OK button. The Select Reverse Out Link - LSR Path list form closes.

v If you choose a numbered outlink interface, configure the Reverse Next Hop parameter.

10 Click on the LSP Path Binding tab to associate the LSR cross-connect path with LER LSPs.

11 Click on the Create button. The LSR Path Binding (Create) form opens.

12 Configure the LSP Path Number parameter.

13 Configure the parameters in the Source LER panel:

- Source TP-LSP ID
- From Node ID
- Source Global ID

14 Configure the parameters in the Destination LER panel:

- Destination TP-LSP ID
- From Node ID
- Source Global ID

15 Click on the OK button. A dialog box appears.

16 Click on the Yes button. The LSR Path Binding (Create) form closes.

17 Click on the OK button. The LSR Path (Create) form closes.

18 Close the Manage MPLS-TP LSPs form.

Procedure 26-8 To create a bidirectional MPLS-TP LSP

A bidirectional LSP consists of MPLS-TP LSPs or LER LSPs that are created on the edge NEs, and the LSR cross-connect—or transit path—that is created on the transit NEs. The 5620 SAM guides you through the creation of the bidirectional MPLS-TP LSP. When the Apply or OK button is disabled, verify that all necessary parameters are configured. When all possible parameters are configured, the 5620 SAM displays a Hint button to provide instructions on the necessary actions.



Note — 5620 SAM guided provisioning is available only for the creation of bidirectional MPLS-TP LSPs. The Hint button does not appear if you are configuring an existing bidirectional MPLS-TP LSP.

1 Choose Manage→MPLS→MPLS-TP LSPs from the 5620 SAM main menu. The Manage MPLS-TP LSPs form opens.

2 Click on the Create button and choose Create Bidirectional TP-LSP. The Bidirectional TP-LSP (Create) form opens with the General tab displayed.

3 Configure the Name parameter.

4 Perform the following to choose an LER A TP-LSP.

i Configure the TP-LSP ID parameter in the LER A panel. The TP-LSP ID parameter is configurable if you disable the TP-LSP ID Auto-Assigned parameter.



Note — The TP-LSP ID must be in the range of the TP-LSP ID Minimum and TP-LSP ID Maximum parameters that you specified in step 3 of Procedure 26-2.

ii Click on the Select button next to the Site ID parameter. The Select Source Site - Bidirectional TP-LSP list form opens.

iii Choose a source site and click on the OK button. The Select Source Site - Bidirectional TP-LSP list form closes and the source site information is refreshed.

5 Perform the following to choose an LER B TP-LSP.

i Configure the TP-LSP ID parameter in the LER B panel. The TP-LSP ID parameter is configurable if you disable the TP-LSP ID Auto-Assigned parameter.



Note — The TP-LSP ID must be in the range of the TP-LSP ID Minimum and TP-LSP ID Maximum parameters that you specified in step 3 of Procedure 26-2.

ii Click on the Select button next to the Site ID parameter. The Select Source Site - Bidirectional TP-LSP list form opens.

iii Choose a source site and click on the OK button. The Select Source Site - Bidirectional TP-LSP list form closes and the source site information is refreshed.

6 Click on the LSP Path tab.

7 Click on the Create button. The Bidirectional TP-LSP Path (Create) form opens with the General tab displayed.

8 Configure the parameters:

- Path Type
- LSP Path Number



Note — You can set the Path Type parameter to Working, and repeat steps 7 to 22 to create a protecting path. You can create one working path and one protecting path.

The LSP Path Number parameter is a global LSP path number that configures the LSP path number on the LER A working and protecting paths, the LER B working and protecting paths, and on the LSR static hop.The LSP Path Number parameter must be the same on all of the hops.

9 Click on the LER A tab.

10 Click on the Select button beside the Out-Link Interface Name parameter. The Select Out-Link - Bidirectional TP-LSP Path list form opens.

11 Click on the Search button. A list of configured routing interfaces (numbered or MPLS-TP unnumbered) appears.

12 Choose a site and click on the OK button. The Select Out-Link - Bidirectional TP-LSP Path list form closes and the Bidirectional TP-LSP Path (Create) form refreshes with the out-link interface information. The 5620 SAM automatically updates the Ingress Label and Egress Label parameters.

13 Click on the Hint button. A window appears displaying an instructional message.

14 Perform one of the following:

a If the message “You have configured the LER-A Out-Link Interface. As a result, 5620 SAM has created the next LSR Path Hop, and has auto-filled the data between the LER-A and the newly created LSR Path Hop.” appears, perform the following steps:

i Click on the LSR Path Hops tab.

ii Choose the LSR path hop with a configuration state of Incomplete and click on the Properties button. The LSR Hop (Edit) form opens.

iii Configure the parameters:

- Display Name
- Reverse Out-Link Interface

iv Click on the OK button. The LSR Hop (Edit) form closes.

v Go to step 16.

b If the message "You have configured the LER-A Out-Link Interface. 5620 SAM is unable to determine the next hop (this could be due to an unconnected cable). As a result, 5620 SAM has enabled the LSR Path Hop creation, and the LER-B Out-Link Interface selection." appears, perform the following:

- If the next hop in the path is not the LER B, go to step 15 to create an LSR path hop.
- If the next hop is the LER B, go to step 16.

c If the message "You have configured the LER-A Out-Link Interface. As a result, 5620 SAM has auto-completed the data between LER-A and LER-B." appears, perform the following steps:

i Click on the OK button to complete the path configuration. The Bidirectional TP-LSP Path (Create) form closes and the Bidirectional TP-LSP (Create) form reappears.

ii Go to step 23.

15 Perform the following to create an LSR path hop:

i Click on the LSR Path Hops tab.

ii Click on the Create button. The LSR Hop (Create) form opens.

iii Configure the Display Name parameter.

iv Click on the Select button beside the Forward Out-Link parameter. The Select Forward Out-Link - Bidirectional TP-LSP Path list form opens.

v Choose an interface and click on the OK button. The Select Forward Out-Link - Bidirectional TP-LSP Path list form closes and the LSR Path Hops (Create) form refreshes with the forward out-link interface information. The 5620 SAM automatically updates the Forward Ingress Label and Forward Egress Label parameters.

vi Click on the Hint button. The message "You have configured the Forward Out-Link Interface. As a result, 5620 SAM has auto-completed the data between this LSR Path Hop and the previous hop on the forward path." appears.

vii Click on the Select button beside the Reverse Out-Link parameter. The Select Reverse Out-Link - Bidirectional TP-LSP Path list form opens.

viii Choose an interface and click on the OK button. The Select Reverse Out-Link - Bidirectional TP-LSP Path list form closes and the LSR Path Hops (Create) form refreshes with the reverse out-link interface information. The 5620 SAM automatically updates the Reverse Ingress Label and Reverse Egress Label parameters.

ix Click on the OK button. The LSR Hop (Create) form closes.

x Click on the Hint button.

xi If the message "You have configured the LSR Path Hop Reverse Out-Link Interface. 5620 SAM is unable to determine the next hop (this could be due to an unconnected cable). As a result, 5620 SAM has enabled the LSR Path Hop creation, and the LER-B Out-Link Interface selection.", perform the following. Otherwise, go to step xiii.

- If the next hop in the path is not the LER B, return to step 15 to create an LSR path hop.
- If the next hop is the LER B, go to step 16.

xii If the message "You have configured the Reverse Out-Link Interface. As a result, 5620 SAM has created the next LSR Path Hop, and auto-completed the data between this LSR Path Hop and the newly created LSR Path Hop." appears, perform the following steps:

- Click on the LSR Path Hops tab.
- Choose the LSR path hop with a configuration state of Incomplete and click on the Properties button. The LSR Hop (Edit) form opens.
- Configure the parameters:
  - Display Name
  - Reverse Out-Link Interface
- Click on the OK button. The LSR Hop (Edit) form closes.
- Go to step 16.

xiii If the message "You have configured the Reverse Out-Link Interface. As a result, 5620 SAM has auto-filled the data between this LSR Path Hop and LER-B." appears, go to step 21.

16 Click on the LER B tab.

17 Click on the Select button beside the Out-Link Interface Name parameter. The Select Out-Link - Bidirectional TP-LSP Path list form opens.

18 Click on the Search button. A list of configured routing interfaces (numbered or MPLS-TP unnumbered) appears.

19 Choose a site and click on the OK button. The Select Out-Link - Bidirectional TP-LSP Path list form closes and the Bidirectional TP-LSP Path (Create) form refreshes with the out-link interface information. The 5620 SAM automatically updates the Ingress Label and Egress Label parameters.

20 Click on the Hint button. The message “You have configured the LER-B Out-Link Interface. As a result, 5620 SAM has auto-completed the data between LER-B and its next hop on the forward path. The path configuration is now complete.” appears. Perform the following steps:

i Click on the OK button to complete the path configuration. The Bidirectional TP-LSP Path (Create) form closes and the Bidirectional TP-LSP (Create) form reappears.

ii Go to step 23.

21 Click on the OK button. A dialog box appears.

22 Click on the OK button. The Bidirectional TP-LSP Path (Create) form closes.

23 Repeat steps 7 to 22 to create a protecting path, if required.

24 Click on the OK button. The Bidirectional TP-LSP (Create) form closes.

25 Create a BFD template on the LER A and LER B. See Procedure 26-3.

26 Create a proactive OAM template on the LER A and LER B. See Procedure 26-4.

27 Close the Manage MPLS-TP LSPs form.

27 — Service tunnels

27.1 Service tunnel overview *27-2*

27.2 IP/MPLS service tunnels *27-3*

27.3 Ethernet (G.8031) tunnels *27-5*

27.4 Ethernet (G.8032) rings *27-7*

27.5 Workflow to configure service tunnels *27-10*

27.6 Workflow to configure Ethernet (G.8032) rings *27-11*

27.7 Configuring service tunnel procedures *27-11*

27.1 Service tunnel overview

A service tunnel is an entity used to uni-directionally direct traffic from one device to another device. The service tunnel is provisioned to use a specific encapsulation method, such as GRE or MPLS, and the services are then mapped to the service tunnel. For instance, multi-NE VLL and VPLS traffic is transmitted using uni-directional service tunnels in this way.

The most common type of tunnel used in 5620 SAM is a Service Distribution Point binding. Service tunnels originate on an SDP on a source NE and terminate at a destination NE. The destination NE directs packets from the service tunnel to the correct service egress interfaces (SAPs) on that device. Services that originate and terminate on the same NE do not require service tunnels, because the same NE is both the source and the destination.

However, because the concept of a tunnel is a logical construct within 5620 SAM, a number of different configurable objects can actually be used as service tunnels, including:

- SDP binding:

  Because SDP bindings can be associated to a service of any type, the service tunnel discovery includes services that are associated to SDP bindings of a given service.
- Service to Tunnel Association:

  Discovery adds tunnels that are associated to a given service.
- Ethernet tunnel (G.8031):

  Discovery adds the global Ethernet Tunnel that the Tunnel Endpoint (SAP's terminating port) is a member of.
- Ethernet ring (G.8032):

  Discovery adds the Ethernet Ring that the Ethernet Element is a member of.
- Ethernet radio ring (G.8032):

  Discovery adds the Ethernet radio ring that the Ethernet Element is a member of. See the *5620 SAM MPR User Guide* for more information.
- PBB:

  Discovery adds the VPLS or MVPLS services which contain the PBB tunnel (B-Sites) of the given Epipe or VPLS.
- P2MP RSVP LSP:

  Discovery adds the P2MP LSPs retrieved from the MVPN LSP Template associated to PIM sites.
- Optical Transport Service:

  Discovery adds optical services that are traversing network interfaces which are being used by an L2/L3 VPN through any static or dynamic LSPs that are bound to SDPs on the service if the following are true:
  - LSPs are bound to service tunnels (SDPs) on the service
  - One or more of the corresponding hops on the LSP active path share the same port with the optical service termination

- Mobile backhaul (applicable to 9500 MPR and 7705 SAR on MPLS-based services running over VLAN):

  Discovery adds MPR VLL services that are associated to an SDP tunnel or are traversing through network interfaces which are being used by an L2/L3 VPN through any static or dynamic LSPs that are bound to SDPs on the service.

The Service Tunnels tab exists on the applicable service configuration forms. This tab lists the objects considered as service tunnels (such as SDPs, Ethernet rings, Ethernet tunnels, other services) that are currently used by the service you are querying. The associated Discover Service Tunnels button removes any previously discovered service tunnels on the service and initiates a manual rediscovery of the tunnels, based on direct usage and current service configurations.

For composite services, the service tunnel discovery action initiates the discovery of service tunnels on the participating services. The listing includes the service tunnels that are currently used by member services.

The Flow-through Services tab is on the configuration forms of the objects that can be used as a service tunnel. The tab lists the other services that are currently using the object you are querying as a service tunnel. The associated Discover Flow-through Services button removes any previously discovered flow-through services and initiates a manual rediscovery of the tunnels, based on direct usage and current service configurations.

For composite services, the concept of using a service as a service tunnel is not supported. The Flow-through Services tab does not appear on the composite service configuration forms.

For fault management, an association type of alarm relationship exists between a service and the service tunnels that the service uses. This allows the service tunnel alarms to propagate up to the service level. These association alarms are displayed on the Alarms on Related Objects tab, under the Faults tab of the service. Because this is a one-way association, service alarms are not propagated to the service tunnels that the service is using.

Tunnel selection profiles

The 5620 SAM uses a tunnel selection profile to assign transport tunnels for a service when the service is configured for automatic SDP binding creation. Tunnel selection profiles can also be used for services when the SDP binding creation is performed manually. The 5620 SAM chooses tunnels and return tunnels when the automatic selection of transport tunnels is enabled and a tunnel selection profile is specified.

A tunnel selection profile contains tunnel administrative groups. When the profile is used within a service to create SDP bindings, any tunnels that include the tunnel administrative group in that profile become eligible for consideration in the tunnel selection process. See chapter 79 for more information about tunnel administrative groups.

27.2 IP/MPLS service tunnels

Distributed service traffic is transported between PE NEs by circuits aggregated in unidirectional service tunnels.

The operational theory of a service tunnel is that the encapsulation of the data between the two managed edge NEs appears as a Layer 2 path to the service data although it is really traversing an IP or IP/MPLS core.

Tunnel policies from older releases of 5620 SAM can be converted to the newer template-based policies by using a “Convert” button located on the rule configuration form. You cannot configure CoS forwarding, LDP-over-RSVP, or multiple LSP bindings on SDP features.

A service tunnel uses GRE or MPLS encapsulation. For MPLS, a mesh of MPLS paths and LSPs must be present in the network core. You associate service tunnels with LSPs during service tunnel configuration. The 5620 SAM supports LSP creation using a basic LDP variant such as T-LDP, or using LDP over RSVP for tunnel-in-tunnel functionality based on traffic classification.

A 5620 SAM operator binds a service site to a service tunnel during service configuration. A service tunnel has a unique ID on an NE and cannot be deleted when it is currently associated with a service.

ACL IP and ACL MAC policy filters for service tunnels contain options for forwarding packets on a specific service tunnel based on matching criteria, as described in chapter 44.

IP/MPLS service tunnels design considerations

Consider the following before you configure IP/MPLS service tunnels:

- Service tunnels are unidirectional, so they are required in both directions between the source NE and the destination NE.
- The tunnel is not specific to one service or one type of service. After a tunnel exists, multiple SDPs can be aggregated over the tunnel. The SDPs can belong to different services and different customers.
- When a tunnel already exists, 5620 SAM does not automatically create a new tunnel, even if the only available tunnel is down. This prevents the creation of multiple inoperable tunnels.
- All services that are mapped to a tunnel use the same transport encapsulation type defined for the tunnel.
- Operations on the tunnel affect all the services that are associated with the tunnel. For example, the operational and administrative states of a tunnel control the state of service circuits that are carried on the tunnel. In the case of LSP-based tunnels, an LSP can be replaced in the tunnel without reconfiguring each service bound to the tunnel.
- A service tunnel is locally unique to an NE. The same tunnel ID can appear on other NEs.
- A service tunnel uses the system IP address to identify the far-end edge NE.
- A service tunnel can be configured using a tunnel template. A user who is assigned the create tunnel template scope of command role can create a tunnel template. The template manager can also apply the tunnel template to a service tunnel. See “Managing templates” in the *5620 SAM Scripts and Templates Developer Guide* for more information about the administrative tasks associated with tunnel templates.
- An SDP tunnel template can be applied to an auto tunnel policy.

See the appropriate device documentation for more detailed information about service tunnels.

Class-based forwarding

Packets of the same CoS and service are forwarded over a specific RSVP LSP (or a static LSP), which is part of an SDP that the service (instance) is bound to. The forwarding decision is based on the forwarding class of the packet, as assigned by the ingress QoS policy defined for the SAP.

When implementing class-based forwarding, consider the following:

- Class-based forwarding is typically implemented using the service tunnel configuration forms, as detailed in Procedure 27-1. Class-based forwarding configurations can also be altered after their initial creation by editing the service tunnel configuration form as detailed in Procedure 27-13.
- An LSP can carry packets of a forwarding class for one service and at the same time, carry packets of a different forwarding class for another service. In other words, the same LSP can be used by more than one SDP, even where the forwarding class assignments are different.
- Within an SDP, only one LSP can support a specific CoS.
- A service instance (or service site) can be bound to SDPs of differing CoS configurations, as well as regular SDPs.
- One LSP in the SDP must be designated as the default LSP. The default LSP is used by the SDP if there is no available LSP that matches the packet's forwarding class. When the default LSP is down, the SDP is also brought down.
- Class-based forwarding can be applied to all services supported by the SRs. For VPLS, you can specify an LSP to forward all multicast/broadcast packets (by default, the default LSP is used). For VLL, shared queuing must be enabled on the ingress SAP to support the class-based forwarding.
- Class-based forwarding is configurable on the 7750 SR, 7710 SR, 7450 ESS, and 7950 XRS.

27.3 Ethernet (G.8031) tunnels

The IEEE 802.1ah Provider Backbone Bridging specification employs Provider MSTP to ensure loop avoidance in a resilient native Ethernet core. With P-MSTP, failover times depend largely on the size of the network and the connectivity model used in the network. MPLS tunnels provide core scaling and fast failover times using MPLS FRR. A service based on native Ethernet backbone achieves the same fast failover times as MPLS FRR.

Core Ethernet tunnels compliant with the ITU-T G.8031 specification achieve 50 ms resiliency for backbone failures. A configured Ethernet tunnel can be selected when configuring an L2 access interface on a B-VPLS.

The 5620 SAM uses two different approaches to configure Ethernet tunnels in the network.

- Approach 1 (recommended):
  5620 SAM provisions an end-to-end Ethernet G.8031 tunnel which reduces configuration errors and aids the diagnosis of any problem in the tunnel. 5620 SAM automatically configures the Ethernet tunnel endpoint and path endpoint on each of the participating NEs. See Procedure 27-5 for more information.

  The Ethernet tunnel and path are network wide objects that provide the following benefits:
  - the Ethernet tunnel provides the aggregated State of the Tunnel and reports any inconsistency in the configuration of the endpoints or paths
  - faster and easier provisioning that allows you to configure common properties such as holdTime and revertTime at the network level and then apply them to each tunnel endpoint
  - 5620 SAM accelerates the creation of global and local MAs, and MEPs by using a continuity check
- Approach 2:
  The 5620 SAM provides the ability to provision Ethernet tunnel endpoints and path endpoints separately on each NE. See Procedure 27-4 for more information on creating Ethernet endpoints. If Ethernet tunnel endpoints are created this way (or discovered from the NE) you can associate them to a network-wide Ethernet tunnel and path, but this must be done manually.



Note — Network-wide Ethernet tunnels and paths are not automatically discovered from the NE.

Transit services

Transit services are supported on the 7210 SAS-D and 7210 SAS-M (in access-uplink mode), Release 4.0 R7 or later, and on the 7210 SAS-T.

Transit services use default QinQ SAPs (which are also called transit SAPs) to forward traffic for data services. Transit SAPs (notation *.*) receive and forward frames with any encapsulation value, and eliminate the need for customer VLAN-specific SAPs on virtual switching instances for service sites with transit SAPs. Data services use transit services for transparent forwarding, which can reduce configuration time and move traffic more efficiently.

Although transit services function as service tunnels, they are managed in the same way as other VPLS and VLL services in the 5620 SAM: they have service IDs, appear as services in navigation trees, contain sites and interfaces, and appear on service topology maps. Properties forms for transit services share the same tab structure and functionality as forms for other services in the 5620 SAM. You can use the Transported Services tab to view and access the data services that use the transit service (you must first discover the services). You can also view and access a transit service that is associated with a VLAN Uplink, using the Transit Services tab on the VLAN Uplink form. You can access VLAN Uplink forms from the service topology map. See "Service topology maps" in section 6.2 for more information.

Any alarms that are generated on a transit service are propagated to the data service that uses the transit service, and appear as alarms on related objects on the Faults tab of the data service properties form.

You can create transit services automatically for VPLS G.8032 Ethernet rings using the Create Transit Services function. See Procedure 27-10 for more information. Transit services created by this method are new services, and contain only transit SAPs. The 5620 SAM creates linked transit SAPs on all sites on the ring.

For non-G.8032 VPLS and VLL services, manually-configured transit SAPs on the services are used as a transit service by the 5620 SAM when the transit SAPs are connected by a physical link.

When you use the Connect to Ethernet Ring function to connect a data service to an Ethernet ring configured with a transit service, the 5620 SAM creates VLAN-specific SAPs for the data service only on the ring site for which Connect to Ethernet Ring is selected. The transit SAPs on the ring transparently forward traffic through other sites on the service.

You can combine transit services using the composite service functionality in the 5620 SAM. Composite services are created automatically when Auto Discover Composite Services is enabled in System Preferences, or manually using the Rediscover Composite Services function. See chapter 74 for more information about composite services.

For more information about transit services and transit SAPs (default QinQ SAPs), including restrictions, see the appropriate NE documentation.

27.4 Ethernet (G.8032) rings

Ethernet Ring Protection (ERP) as specified in ITU-T G.8032, is a protection mechanism for Ethernet ring topologies that provides a resilient Ethernet network. ERP provides sub-50ms protection and recovery switching for Ethernet traffic in a ring topology, and, at the same time, ensures that loops are not formed at the Ethernet layer. G.8032v1 supports a single ring topology; G.8032v2 supports multiple rings/ladder topology. For more information about Ethernet (G.8032) rings, see the ITU website at http://itu.int.

ERP topology

An ERP topology is a collection of Ethernet ring nodes that forms a closed physical loop. Between two and sixteen Ethernet ring nodes are supported per ERP topology. One ERP topology is supported per NE. Up to two ERP instances are supported per ERP topology. Ethernet ring links connect two adjacent Ethernet ring nodes participating in the same ERP topology.

Loop avoidance in the ring is achieved by guaranteeing that at anytime, traffic may flow on all but one of the ring links. This link is called the ring protection link (RPL). One designated node, the RPL Owner (also referred to as the master node), is responsible to block traffic over the RPL.

Supported ERP service types

You can configure the following service types in an ERP (G.8032) topology using the 5620 SAM on the following NEs:

- VPLS. VPLS that support ERP SAPs can connect to other rings and Ethernet services using VPLS SAPs. A VPLS can use a single ring (main or sub-ring) or multiple rings.
  - 7210 SAS 3.0 or later devices, except the 7210 SAS-X 24F 2XFP, Release 3.0 R1; Release 3.0 R2 and later support ERP
- VLAN service
  - OS 6400, OS 6850, OS 6850E, OS 6855, OS 9700E, OS 9800E, Release 6.4.4 or later
  - OS 6250M, Release 6.6.2 or later
  - OS 6450, Release 6.6.3 or later
  - 9500 MPR, Release 3.1 or later; see the *5620 SAM MPR User Guide* for more information.
- VLL service (Cpipe and Epipe services only)
  - 9500 MPR, Release 3.1 or later, see the *5620 SAM MPR User Guide* for more information.



Note — For OmniSwitch NEs, only the Ethernet ring element configuration (and not Ethernet ring) is supported on the 5620 SAM. See Procedure 27-7 for more information.

Automatic Ethernet ring creation

The 5620 SAM automatically unites Ethernet ring elements in the network into Ethernet rings, and creates path objects to link endpoints within the ring. In order for the 5620 SAM to create an Ethernet ring, the following must exist:

- at least two Ethernet ring elements with path endpoints
- a physical link between the endpoints

The 5620 SAM detects the ring elements and the physical link, then creates an Ethernet ring to contain the ring elements, and path objects to link them. If one of the ring elements is already part of an Ethernet ring, then the other element is added to the existing ring. If both elements are part of existing rings, then the rings are merged (see "Merging Ethernet rings" below).

Automatic Ethernet ring creation is triggered by the following events:

- creation or detection of a path endpoint on an Ethernet ring element
- creation or detection of a physical link between two path endpoints on Ethernet ring objects
- performance of a global Ethernet ring audit (see "Auditing Ethernet rings")

The 5620 SAM also detects and creates Ethernet sub-rings, and creates interconnects between rings and sub-rings when appropriate. You can view the sub-rings associated with a ring in the Sub-Rings tab of the Ethernet ring configuration form.

See Section 27.6 for information about using the 5620 SAM to automatically create Ethernet rings.

You can manually create Ethernet (G.8032) rings using the 5620 SAM GUI or using the OSS service provisioning client. See Procedure 27-8 to create Ethernet (G.8032) rings using the 5620 SAM GUI. See "MPLS, LSP, and service tunnel configuration" in the *5620 SAM XML OSS Interface Developer Guide* for information about configuring Ethernet (G.8032) rings using the OSS client application.

Merging Ethernet rings

When the 5620 SAM detects a physical link between two Ethernet ring element path endpoints on separate Ethernet rings, the rings are automatically merged together. One of the Ethernet rings is deleted, and the elements and paths from that ring are added to the other ring. The following criteria are used to determine which ring is deleted:

- If one of the rings was created manually using the 5620 SAM, then the other ring is merged into the manually-created ring.
- If both rings were created manually, then the smaller ring is merged into the larger ring, based on the number of Ethernet ring elements.
- If both rings were created automatically, then the smaller ring is merged into the larger ring, based on the number of Ethernet ring elements.
- If the rings have the same number of elements, and were both created the in the same manner, then the ring with the higher Manager ID is merged into the other ring.

Auditing Ethernet rings

You can use the 5620 SAM to perform a global or local audit of an ethernet ring. An audit can find missing elements, paths, and interconnects, and potentially merge rings if a link is found. When an audit discovers a problem that cannot be resolved, an alarm is raised against the ethernet ring, and the problems encountered by the audit are displayed in the alarm details. Performing another audit clears the alarm, if the problems have been resolved.

Procedure 27-16 describes how to audit Ethernet rings. Performing a global Ethernet ring audit both creates and merges Ethernet rings, even if automatic Ethernet ring creation is disabled.

Service provisioning on Ethernet (G.8032) rings

The 5620 SAM accelerates the provisioning of VPLS instances on Ethernet (G.8032) rings by automatically creating the control services and data services on the rings. Services are configured on Ethernet (G.8032) rings in the same method as service tunnels.

You can automatically configure transit services on VPLS G.8032 Ethernet rings. See "Transit services" in section 27.3 and Procedure 27-10 for more information.

You can create Ethernet (G.8032) rings using the 5620 SAM GUI or using the OSS service provisioning client. See Procedure 27-8 to create Ethernet (G.8032) rings using the 5620 SAM GUI. See "MPLS, LSP, and service tunnel configuration" in the *5620 SAM XML OSS Interface Developer Guide* for information about configuring Ethernet (G.8032) rings using the OSS client application.

27.5 Workflow to configure service tunnels

1. Before you can create an MPLS service tunnel, you must create a static or dynamic LSP. See Procedure 25-6 for static LSPs. See Procedure 25-8 for dynamic LSPs.
2. Create an IP/MPLS service tunnel and assign it to an NE as follows:
   a. Create an IP/MPLS service tunnel; see Procedure 27-1.
   b. Create an IP/MPLS service tunnel using a tunnel template. See Procedure 27-2.



Note — Service tunnels are unidirectional, so they are required in both directions between the source NE and the destination NE.

   c. Create a tunnel administrative group and a tunnel selection profile and assign the tunnel selection profile to an SDP binding. See Procedure 79-1 and Procedures 27-1 and 27-3 for more information.
3. Perform one of the following to create an Ethernet service tunnel:
   a. Create an Ethernet service tunnel endpoint. See Procedure 27-4.
   b. Create an Ethernet service tunnel and assign endpoints to the tunnel. See Procedure 27-5.
4. Create transit services on Ethernet rings as required. See Procedure 27-10.
5. As required, discover and list service tunnel information. See Procedures 27-11 and 27-12.
6. Perform one of the following to view service tunnel information:
   a. View and manage service tunnels and tunnel elements. See Procedure 27-13.
   b. View the service tunnel topology. See Procedure 27-14.
7. As required, run an OAM validation test on a service tunnel. See Procedure 27-15.

27.6 Workflow to configure Ethernet (G.8032) rings

1 Perform one of the following to create Ethernet ring elements:

   a Create an Ethernet ring element for all supported devices except for OmniSwitch and 9500 MPR devices. See Procedure 27-6 for more information.

   b Create an Ethernet ring element for an OmniSwitch. See Procedure 27-7.

   c Create an Ethernet radio ring element for an 9500 MPR. See the *5620 SAM MPR User Guide* for more information.

2 Perform one of the following to create physical links:

   a Configure LLDP to automatically discover and create physical links. See "LLDP" in Chapter 22 for information about using LLDP.

   b Manually create a physical link. See Procedure 6-33.

3 If required, perform a global Ethernet ring audit to trigger Ethernet ring creation and mergers. See Procedure 27-16.

27.7 Configuring service tunnel procedures

Procedure 27-1 describes how to create an IP/MPLS service tunnel.

Procedure 27-1 To create an IP/MPLS service tunnel

Before you can create an MPLS service tunnel, you must create a static or dynamic LSP. See Procedure 25-6 for statics LSPs. See Procedure 25-8 for dynamic LSPs.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form opens.

2 Click on the Create button and choose IP/MPLS Service Tunnel (SDP). The IP/MPLS Service Tunnel (SDP) step form opens with the Name & Describe Service Tunnel (SDP) step displayed.

3 Configure the parameters:

- Name
- Description
- Auto-Assign ID
- ID



Note 1 — If a range policy is applied to a service tunnel, a grey text box appears beside the ID parameter to indicate that a range policy is in effect.

Note 2 — If a format policy is applied to a service tunnel, a combo box appears beside the object field during object creation to indicate that a format policy is in effect. When there is only one matching policy, the combo box is dimmed. When there are multiple matching policies, use the combo box to choose a policy. The sequence of the options in the combo box are ordered by the policy Priority parameter.

4 Click on the Next button. The Pick Source Node step is displayed.

5 Perform one of the following to configure the Source Site ID parameter:

a Choose an NE from the list.

i Click on the Select button. The Select a Network Element - Pick Source Node form opens.

ii Choose an NE in the list and click on the OK button. The Select a Network Element - Pick Source Node form closes and the Create Service Tunnel (SDP) form displays the source NE IP address.

b Enter the NE IP address.

6 Click on the Next button. The Pick Destination Node step is displayed.

7 If you are creating an SDP tunnel using MPLS-TP, perform the following. Otherwise, go to step 8.

i Enable the MPLS-TP Far-End parameter.

ii Click on the Select button next to the MPLS-TP Node ID. The Select... form opens with a list of NEs on which MPLS-TP is enabled.

iii Choose an NE and click on the OK button. The Select... form closes.

8 Perform one of the following to configure the Destination Site ID parameter:

a Choose an NE from the list.

i Click on the Select button. The Select a Network Element - Pick Destination Node form opens.

ii Choose an NE in the list and click on the OK button. The Select a Network Element - Pick Destination Node form closes and the Create Service Tunnel (SDP) form displays the destination NE IP address.

b Enter the NE IP address.

9 Click on the Next button. The Specify Transport step is displayed.

10 Perform one of the following:

a For GRE service tunnels:

i Specify GRE for the Underlying Transport parameter.

ii Configure the Signaling parameter.

iii Go to step 20.

b For MPLS service tunnels:

i Specify MPLS for the Underlying Transport parameter.



Note 1 — If the source or destination site is a 7210 SAS-M24F, 7210 SAS-M24F2XFP or 7210 SAS-M24F2XFP [ETR], you cannot configure the Underlying Transport parameter. The devices support only MPLS with TLDP signaling, LDP is not enabled.

Note 2 — When you implement class-based forwarding or specify a transport destination address, you must choose MPLS as the Underlying Transport parameter.

Note 3 — When you specify a transport destination address, you cannot implement class-based forwarding.

Note 4 — When you configure a service tunnel with a source site that is a 7705 SAR, you can choose IPv4 as the Underlying Transport parameter if the destination site is also a 7705 SAR, a GNE, or an unmanaged IP address.

ii Configure the parameters:

- Mixed Lsp Mode
- Revert Time (seconds)
- Ldp Enabled
- Enable BGP-Tunnel
- Signaling

The Revert Time (seconds) parameter appears when the Mixed Lsp Mode parameter is set to true.



Note 1 — When you implement class-based forwarding, you must use one of the following parameter configurations:

- Set Mixed Lsp Mode to true.
- Set Mixed Lsp Mode, Ldp Enabled, and Enable BGP-Tunnel parameters to false.

Note 2 — When you specify a transport destination address, you must use the following parameter configurations:

- Set Ldp Enabled to true.
- Set Mixed Lsp Mode and Enable BGP-Tunnel to false.

Note 3 — You cannot set Enable BGP-Tunnel to true when Ldp Enabled or Mixed Lsp Mode is set to true.

Note 4 — You cannot create a BGP or an LDP tunnel when an LSP exists between the source and destination NEs you specified in steps 4 and 8 respectively.

iii If you set the Ldp Enabled parameter to true, go to step 18.

iv If you set the Enable BGP-Tunnel parameter to true, go to step 20.

11 Click on the Next button. The Specify Class Forwarding step is displayed.

12 Configure the parameters:

- Class Forwarding Capability
- Administrative State
- Enforce Diff-Serv Lsp-Fc Map



Note — When the Class Forwarding Capability parameter is set to Off, the existing class-forwarding configurations are removed.

The Administrative State and Enforce Diff-Serv Lsp-Fc Map parameters are configurable when the Class Forwarding Capability parameter is set to On.

13 Click on the Next button. The Associate LSPs step is displayed.

14 Click on the Add button to bind an LSP to the service tunnel. The Bind LSPs to Service Tunnel form opens with the Bind LSP to Service Tunnel Stage step displayed.

15 Choose an LSP and click on the Finish button.

16 Click on the Close button. The Bind LSPs to Service Tunnel form closes and the LSP is listed on the Create Service Tunnel (SDP) form.

17 If you are enabling class-based forwarding on the LSP:

i Choose an LSP from the list and click on the Set As Default LSP button. This is mandatory. The Default LSP Name appears in the associated field.

ii For a VPLS, specify an LSP to forward all multicast/broadcast packets. Otherwise, the default LSP is used. If the LSP is specified, the Multicast LSP Name appears in the associated field.

iii For any LSPs used for class-based forwarding (including the default), choose the LSP from the list and click on the Choose a Forwarding Class button. Choose the required forwarding class from the contextual menu, which then appears in the Forwarding Class to LSP Mappings table.

18 Click on the Next button. The Specify Transport Destination Address step is displayed.



Note — This step appears if you set the Underlying Transport parameter to MPLS in step 10 and set the Ldp Enabled parameter to true.

19 Configure the Transport Destination Address parameter.

20 Click on the Next button. The Specify Hello Parameters step is displayed.

21 Configure the parameters:

- Keep-Alive Enabled
- Hello Time
- Hello Request Timeout
- Max Drop Count
- Hello Message Length
- Hold Down Time

22 Click on the Next button. The Specify MTU Values step is displayed.

23 Configure the parameters:

- Administrative MTU
- Advertised MTU Override

24 Click on the Next button. The Specify Metric step is displayed, if applicable.

25 Configure the Metric parameter, if applicable.

26 Click on the Next button. The VC Type Related Parameters step is displayed, if applicable.

27 Configure the VLAN VC Ethertype parameters, if applicable.

28 Click on the Next button. The Specify Initial State step is displayed.

29 Configure the Administrative parameter.

30 Click on the Next button. The Booking Factor step is displayed.



Note — This step appears if you set the Underlying Transport parameter to MPLS in step 10 and set the Ldp Enabled parameter to false.

31 Configure the SDP Bandwidth Booking Factor (%) parameter.

32 Click on the Next button. The Associate Service step is displayed.

33 Click on the Select button. The Select Associated Service form opens.

34 Choose a service from the list and click on the OK button. The Select Associated Service form closes. The Associated Service Name and Associated Service ID are updated.

35 Click on the Next button. The Admin Groups step is displayed.

36 Select the tunnel administrative groups in the Unassigned list that you want to assign to the tunnel and click the right arrow to move them into the Assigned list.

37 Click on the Next button. The Network Domain step is displayed.

38 Click the Select button. The Select Network Domain form opens.

39 Choose a network domain from the list and click on the OK button. The Select Network Domain form closes. The Name field is updated.



Note — All SDPs are associated with a network domain. This association is done during the creation or when editing an SDP in the Tunnel (Edit) form. You can also modify the network domain in the Tunnel (Edit) form. See step 57. The Egress Interfaces Consistency State status specifies if all the interface associations to SDP belong to a particular domain.

40 Perform one of the following:

- **a** If you specified MPLS for the Underlying Transport parameter in step 10, click on the Next button and go to step 41.
- **b** If you did not specify MPLS for the Underlying Transport parameter in step 10, click on the Next button and go to step 54.

41 The Port Binding step is displayed.

42 Click on the Select button. The Select Port form opens.

43 Choose an Ethernet or HSMDA port, or a LAG from the list and click on the OK button. The Select Port form closes.



Note — Only ports in hybrid mode or a LAG that contains hybrid ports can be selected.

44 Click on the Next button. The Configure PW Ports step is displayed.

45 Click on the Create button. The PW Port Binding (Create) form opens.

46 Click on the Select button in the PW Port ID panel. The Select PW Port ID - PW Port Binding form opens.

47 Perform one of the following:

a Choose an existing PW port from the list and click on the OK button. The Select PW Port ID - PW Port Binding form closes. Go to step 52.

b Click on the Create button. The PW Port (Create) form opens.

48 Configure the parameters:

- PW Port ID
- Auto-Assign ID
- Encapsulation Type

49 Configure node redundancy for the PW port, if required.

i Click on the Node Redundancy button. The Manage Node Redundancy form appears, preconfigured for MC peer groups.

ii Click on the Search button and configure an existing MC peer group, or click on the Create button and configure a new MC peer group. See Procedure 36-1.

The Node Redundancy button allows you to access the MC sync group configuration within the MC peer group in order to add PW port sync tags.

50 Click on the OK button. The PW Port (Create) form closes.

51 Choose the created PW port from the list and click on the OK button. The Select PW Port ID - PW Port Binding form closes.

52 Configure the parameters:

- VC ID
- Administrative State
- VC Type
- VLAN VC Tag
- Egress Shaper Virtual Port Name
- Intermediate Destination ID
- PW SAP Secondary Shaper

53 Click on the OK button. The PW Port (Create) form closes.

The PW port can also be used in the Service Access Points of the following service types:

- VPRN (see Procedure 29-6)
- IES (see Procedure 29-6)
- VPLS Capture (see Procedure 65-28)

Refer to the specific service chapter and forms when creating the required service access points. Specify the PW port as the Terminating Port when you create these service access points.

The PW port can also be specified as the terminating port for L3 access interfaces of the following service types:

- VPRN (see Procedure 71-22)
- IES (see Procedure 70-17)

The service access point and L3 access interface you create will appear in the lists on the Service Access Points and L3 Access Interfaces tabs of the PW Port (Edit) form.

54 Click on the Finish button to save the configuration. The 5620 SAM prompts you to view the service tunnel configuration.

55 Enable the View the newly created tunnel parameter to view the service tunnel configuration after closing the form, if required.

56 Click on the Close button. The Create Service Tunnel (SDP) form closes.

57 If the View the newly created tunnel parameter in step 55 is enabled, the Tunnel (Edit) form opens with the newly-created service tunnel configuration displayed.

i View or modify the configuration, if required.

ii Click on the Create a template button, if required. See "XML API template script format" in the *5620 SAM Scripts and Templates Developer Guide* for information about creating a template.

iii Close the Tunnel (Edit) form.

58 Close the Manage Service Tunnels form.

Procedure 27-2 To create an SDP using a tunnel template

Before you can create an SDP from a tunnel template, you must create the SDP tunnel template. For more information about creating SDP tunnel templates, see "Managing templates" in the *5620 SAM Scripts and Templates Developer Guide*.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels search form opens.

2 Click on the Create from Template button. A Create Service Tunnel From Template form opens with a list of previously configured SDP tunnel templates.

3 Choose a tunnel template from the list.

4 Click on the OK button. A Create Tunnel from Template form opens with the General tab displayed.

5 Configure the parameters:

- Name
- Description
- Auto-Assign ID
- ID
- Underlying Transport
- PBB Ethernet Type
- Ldp Enabled
- Signaling
- Source Site ID
- Destination Site ID
- Transport Destination Address
- Administrative
- Administrative MTU
- Advertised MTU Override
- Metric
- VLAN VC Ethertype
- No VLAN VC Ethertype

6 Click on the SDP Bandwidth tab. Configure the SDP Bandwidth Booking Factor (%) parameter.

7 Click on the Maintenance tab and configure the following parameters:

- Keep-Alive Enabled
- Hello Time
- Hello Message Length
- Hello Request Timeout
- Hold Down Time
- Max Drop Count

8 Click on the Accounting tab.

9 Click on the Select button beside the Accounting Policy parameter to assign an accounting policy to the service tunnel. A Select Policy form opens with a list of accounting policies.

10 Choose a policy from the list and click on the OK button. The Select Policy widow closes and the Accounting Policy parameter is updated

11 Click on the OK button. The Create SDP from Template form closes.

12 When the Show Created Object parameter is enabled on the template, the Tunnel (Edit) form opens. Close the Tunnel (Edit) form.

Procedure 27-3 To create a tunnel selection profile

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form opens.

2 Click on the Create button and choose Tunnel Selection Profile. The Tunnel Selection Profile (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Profile Name
- Description
- Transport Type
- Multi-Segment Tunnel Selection
- Redundant Path Selection

4 Specify an SDP binding template in the profile, if required. Perform the following.



Note — An SDP binding template allows the 5620 SAM to use the configuration information contained in the template for the automatic creation of SDP bindings. See "Managing templates" in the *5620 SAM Scripts and Templates Developer Guide* for information about creating a template.

i Click on the Select button in the SDP Binding Template panel. The Select SDP Binding Template form opens.

ii Specify a filter, if required, and click on the Search button. A list of SDP binding templates appears.

iii Choose an SDP binding template from the list and click on the OK button. The Tunnel Selection Profile (Create) form is refreshed with the SDP binding template information.

5 Click on the Tunnel Admin Groups tab.

6 Click on the tunnel administrative groups that you want to include in the profile in the Included Admin Groups-Unassigned panel. You can choose multiple groups by holding down the CTRL key when you click on the group.

7 Click on the right arrow to move the selected administrative groups to the Included Admin Groups-Assigned panel. You can move an assigned administrative group to the unassigned portion of the form, if required, by choosing the group and clicking on the left arrow.

8 Click on the tunnel administrative groups that you want to exclude from the profile in the Excluded Admin Groups-Unassigned panel. You can choose multiple groups by holding down the CTRL key when you click on the group.

9 Click the right arrow to move the selected administrative groups to the Excluded Admin Groups-Assigned panel. You can move an assigned parameter to the unassigned portion of the form, if required, by choosing the group and clicking on the left arrow.

10 Click on the OK button. The Tunnel Selection Profile (Create) form closes.

11 Close the Manage Service Tunnels form.

Procedure 27-4 To create or configure an Ethernet tunnel endpoint

Before you can create an Ethernet tunnel, you must configure the Ethernet tunnel endpoint.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels search form opens.

2 If you are configuring an existing Ethernet Tunnel Endpoint, go to step 8.

3 Click on the Create button.

4 Click on Ethernet Tunnel Endpoint from the contextual menu. The Select Network Elements form opens.

5 Choose a site on which to create an Ethernet tunnel endpoint.

6 Click on the OK button. The Ethernet Tunnel Endpoint (Create) form opens with the General tab displayed.

7 Go to step 10.

8 Select Ethernet Tunnel Endpoint (Ethernet Tunnel) on the drop-down menu in the Manage Service Tunnels form. Click on the Search button to display a list of the existing endpoints.

9 Select the endpoint you want to configure and click on the Properties button.

The Ethernet Tunnel Endpoint (Edit) form opens with the General tab displayed.

10 Configure the following parameters:

- Tunnel Endpoint ID
- Site ID
- Protection Type
- Encap Type
- Administrative State
- Hold Time Down
- Hold Time Up (deciseconds)
- Revert Time (seconds)
- Access Adapt QoS
- Enable Per Forwarding Path Ingress Queue
- Operational Path Endpoint Threshold
- Description
- Configured MAC Address

The Tunnel Endpoint ID and Site ID are only configurable when you are creating a new Ethernet Tunnel Endpoint.

The Access Adapt QoS, Enable Per Forwarding Path Ingress Queue, and Operational Path Endpoint Threshold parameters are only displayed when the Protection Type is set to Load Sharing.

11 Click on the Path Endpoints tab to configure the Path Endpoints.

12 Perform one of the following:

a If you are configuring an existing Ethernet Tunnel Path Endpoint, select the required path endpoint from the list and click Properties. The Ethernet Tunnel Path Endpoint (Edit) form opens with the General tab displayed.

b If you are configuring a new Ethernet Tunnel Path Endpoint, click on the Create button. The Ethernet Tunnel Path Endpoint (Create) form opens with the General tab displayed.

13 Configure the following parameters for each Path Endpoint.

- Path ID
- Description
- Administrative State
- Precedence
- APS Command

The Path ID parameter is only configurable when you are creating a new Ethernet Tunnel Path Endpoint.

The APS Command parameter is only displayed and configurable when you are configuring an existing Ethernet Tunnel Path Endpoint and when the Protection Type parameter you configured in step 10 is set to G8031 1:1. The associated "Perform APS Command" button is used to perform the selected command on the path endpoint.

14 Click on the Properties button in the Ethernet Path panel if you need to view or alter parameters on the Ethernet Path or configure a CFM Test. The Ethernet Path - Properties button is only displayed and selectable when you are configuring an existing Ethernet Tunnel Path Endpoint.

15 If you are configuring an existing Ethernet Tunnel Path Endpoint, go to step 23.

16 Click on the Port tab.

17 Click on the Select button. The Select Member Port form opens.

18 Click on the Search button to list the available ports. Choose the port to use for the Ethernet tunnel path endpoint.

19 Click on the OK button. The Ethernet Tunnel Path Endpoint (Create) form displays the selected member port.

20 Configure the parameters:

- Control Tag (Outer Encapsulation Value)
- Control Tag (Inner Encapsulation Value)

21 Click on the OK button. The Ethernet Tunnel Path Endpoint (Create) form closes and the Path Endpoints tab displays the new Ethernet Tunnel Path Endpoint in the list.

22 Go to step 30.

23 Click on the MEPs tab, if you need to create a MEP for the existing Ethernet Tunnel Path Endpoint. Otherwise go to step 30.

24 Click on the Create button. The MEP (Create) form opens with the General tab displayed.

25 Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Control MEP
- Control Sap Tag
- Low-priority Defect
- MAC Address
- Fault Propagation
- Type
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)
- CCM Padding Packet Size (Bytes)

The Control MEP parameter is only displayed if the Interface Type parameter is set to Ethernet Tunnel Path Endpoint.

The Control Sap Tag parameter is only configurable on a 7210 SAS-M Release 4.0 R2 and later, or a 7210 SAS-X Release 4.0 R2 and later.

The CCM Padding Packet Size (Bytes) parameter cannot be configured when the CCM interval parameter is set to 10 ms or 100 ms.



Note — When configuring a Down MEP on a Subscriber Group Interface SAP, the Direction parameter cannot be configured.

26 If the Maintenance Domain for this MEP has a Name Type of none and its Maintenance Association has a Name Format of icc-based, then the Y.1731 TEST and the AIS tabs will also be displayed. See Procedure 65-26 for more information.

27 Click on the OK button. A dialog box appears.

28 Click on the OK button. The MEP (Create) form closes and the newly-created MEP is displayed in the list on the MEPs tab.

29 Click on the OK button. The Ethernet Tunnel Path Endpoint (Edit) form closes and the Path Endpoints tab displays the available Ethernet Tunnel Path Endpoints in the list.

30 Repeat steps 12 to 29 for any other Ethernet Tunnel Path Endpoints you need to create or configure.

31 Click OK. A dialog box appears.

32 Click Yes to close the Ethernet Tunnel Endpoint form.

Procedure 27-5 To create an Ethernet tunnel

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels search form opens.

2 Click on the Create button.

3 Click on Ethernet Tunnel from the contextual menu. The Ethernet Tunnel (Create) form opens.

4 Configure the following parameters:

- Tunnel ID
- Name
- Description
- Protection Type
- Encap Type
- Hold Time Down
- Hold Time Up (deciseconds)
- Revert Time (seconds)
- Access Adapt QoS
- Enable Per Forwarding Path Ingress Queue
- Operational Path Endpoint Threshold

The Access Adapt QoS, Enable Per Forwarding Path Ingress Queue, and Operational Path Endpoint Threshold parameters are only displayed when the Protection Type is set to Load Sharing.

5 Click on the Apply button. The Ethernet Tunnel (Edit) form opens with the General tab displayed.

6 Click on the Components tab. Right click on Tunnel Endpoints and choose one of the following from the contextual menu.

a Create Ethernet Tunnel Endpoint.

i Refer to Procedure 27-4 to create an Ethernet Tunnel Endpoint. The endpoint will be listed as Endpoint A on the Ethernet Tunnel form in the Tunnel Endpoints Section.



Note — The parameter values specified in step 4 are automatically applied in the Ethernet Endpoint form when creating an endpoint.

ii Repeat step i to create Endpoint B.

iii Go to step 7.

b Add Existing Endpoint.

i The Select Endpoints form opens.

ii Click on the Search button and select an endpoint.

iii Click OK.

iv The endpoint is listed as Endpoint A on the Ethernet Tunnel form in the Tunnel Endpoints Section.



Note — The parameter values specified in step 4 are not automatically applied to the selected Ethernet endpoint.

v Repeat steps i to iv to select Endpoint B.

7 Right click on Paths and choose Create Ethernet Paths from the contextual menu to create a path. The Ethernet Path (Create) form opens with the General tab displayed.

8 Configure the parameters:

- Auto-Assign ID
- ID
- Description

9 Click on the Endpoints tab. Perform one of the following:

a Manually configure the following parameters for endpoints A and B.

- Site ID
- Path ID
- Precedence
- Administrative State
- Control Tag (Outer Encapsulation Value)
- Control Tag (Inner Encapsulation Value)
- Member Port



Note — A path endpoint cannot be administratively enabled if one of the following is true:

- An operationally up same-fate SAP on the Ethernet tunnel endpoint does not have a tag configured for the path endpoint.
- The Control Tag (Outer Encapsulation Value), Control Tag (Inner Encapsulation Value), and Member Port parameters are not configured.

b Perform the following steps to specify a path endpoint for endpoints A and B.

i Click on the Select button beside the Path ID parameter. The Select Path Endpoint form opens.

ii Click on the Search button and select an available endpoint.

iii Click OK. The endpoint parameters are automatically populated.



Note — To delete an Ethernet tunnel path endpoint, click on the Search button to display a list of endpoints, select an endpoint, then click on the Delete button.

10 Click on the Intermediate Services tab to view and specify the intermediate services for the Ethernet path. The services that you add to the list (or that already appear there) are in the order of proceeding from Endpoint A to Endpoint B. Perform the following to add an intermediate service:

i Click on the Create button. The Select Service form opens.

ii Click on the Search button to display a list of intermediate services available to include in this path. Only VLL services can be included.

iii Select the required service and click on the OK button.

The Select Service form closes and the service you chose is displayed in the list on the Intermediate Services tab.



Note — 5620 SAM does not perform a validation to confirm whether the selected service is actually along the path between the two path endpoints.

iv Repeat steps i to iii to add another intermediate service, if required.



Note 1 — If you have an intermediate service highlighted in the list and want to add another service immediately above it, click on the Insert Component button rather than the Create button. The Create button places an additional service at the bottom of the list, whereas the Insert Component button places it directly above a highlighted service.

Note 2 — You can change the ordering of intermediate services in the list by selecting a particular service and using the Move Up or Move Down buttons.

11 Click on the CFM Continuity Check tab to configure a CFM Continuity Check test for each path.

It is mandatory to have the following steps completed before selecting a test:

- Create a Maintenance Domain. The Name Type must be None. See chapter 78 for more information.
- Create a CFM Continuity Check Test. See Procedure 32-6 for information.

12 Click on the Select button. The Select CFM Test form opens.

13 Click on the Search button to list the available CFM tests. Choose a CFM test.

14 Click on the OK button. The CFM Test is listed and the MEP Auto Creation check boxes are enabled.

15 Perform one of the following:

a Enable one of the MEP Auto Creation buttons:

i Click on the Run Continuity Check Protocol button to create Maintenance Associations and local and remote MEPs. Any existing Remote MEPs that do not match the local MEPs are deleted. MEPs are turned up and CCM Messages are enabled, and the control MEP property is set on the MEPs.

ii Click on the Create MEPs button to create local MEPs. Any existing Remote MEPs that do not match the local MEPs are deleted.

b Continue to step 16 and select the Run Continuity Check Protocol button or Create MEPs button at a later date.

16 If required, click on the MEP tab to display the MEP form and select the check box to set the Control MEP parameter.

17 Click on the OK button. The Ethernet Tunnel form is displayed with the new Path information.

18 If the Protection Type parameter in step 4 was set to G8031 1:1, then repeat steps 7 to 17 for the other path.

19 If the Protection Type parameter in step 4 was set to Load Sharing, then repeat steps 7 to 17 for all paths.

20 Click Apply. The Path Id, Operational State, and CC Protocol State are updated and the path endpoints with this specific configuration are sent to the NEs.



Note — The CC protocol state appears under the global path (in the navigation tree and on the CFM Continuity Check form). The CC protocol state displays the state of the continuity check protocol running between the MEPs of the two endpoints of the path.

21 Click OK. A dialog box appears.

22 Click Yes to close the Ethernet Tunnel (Create) form.

Procedure 27-6 To create or configure an Ethernet Ring Element

This procedure describes how to create a new Ethernet Ring Element or configure an existing one.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels search form opens.

2 If you are configuring an existing Ethernet Ring Element, go to step 8.

3 Click on the Create button.

4 Click on Ethernet Ring Element from the contextual menu.

5 Choose a site from the Select Network Elements form to create an Ethernet Ring Element.



Note — You can create multiple ring elements at this point if you select more than one site here.

6 Click on the OK button. The Ethernet Ring Element (Create) form opens with the General tab displayed.

7 Go to step 10.

8 Select Ethernet Ring Element (Ethernet Ring) on the drop-down menu in the Manage Service Tunnels form. Click on the Search button to display a list of the existing ring elements.

9 Select the ring element you want to configure and click on the Properties button.

The Ethernet Ring Element (Edit) form opens with the General tab displayed.

10 Configure the following parameters:

- ID
- Auto-Assign ID
- Site ID
- Description
- Administrative State
- Compatible Version
- CCM Hold Time Down (deciseconds)
- CCM Hold Time Up (deciseconds)
- Guard Time (deciseconds)
- Revert Time (seconds)
- Ring Protection Link Type
- Ring Node ID

The ID and Site ID are only configurable when you are creating a new Ethernet Ring Element.

11 Configure the parameters for a sub-ring, if required:

- Type
- Ethernet Ring ID
- VPLS
- Propagate Topology Change

12 Click on the Path Endpoints tab to configure the Path Endpoints.

13 Perform one of the following:

a If you are configuring an existing Ethernet Ring Path Endpoint, select the required path endpoint from the list and click Properties. The Ethernet Ring Path Endpoint (Edit) form opens with the General tab displayed.

b If you are configuring a new Ethernet Ring Path Endpoint, click on the Create button. The Ethernet Ring Path Endpoint (Create) form opens with the General tab displayed.

14 Configure the following parameters for each Path Endpoint.

- Path ID
- Description
- Administrative State
- Path Endpoint Type

The Path ID parameter is only configurable when you are creating a new Ethernet Ring Path Endpoint.

15 If configuring an Ethernet Ring Path Endpoint on a 7210 SAS-M Release 4.0 R2 and later, or a 7210 SAS-X Release 4.0 R2 and later, configure the Switch Command parameter and click on the Perform Switch Command button.

16 If you are configuring an existing Ethernet Ring Path Endpoint, go to step 24.

17 Click on the Port tab.

18 Click on the Select button. The Select Member Port form opens.

19 Click on the Search button to list the available ports. Choose the port to use for the Ethernet ring path endpoint.

20 Click on the OK button. The Ethernet Ring Path Endpoint (Create) form displays the selected member port.

21 Configure the parameters:

- R-APS Tag (Outer Encapsulation Value)
- R-APS Tag (Inner Encapsulation Value)

22 Click on the OK button. The Ethernet Ring Path Endpoint (Create) form closes.

The Path Endpoints tab displays the new Ethernet Ring Path Endpoint in the list.

23 Repeat steps 3 to 22 for the other Ethernet Ring Path Endpoint you need to create, if required.

24 Click OK. A dialog box appears.

25 Click Yes to close the Ethernet Ring Element form.

Procedure 27-7 To create or configure an Ethernet Ring Element on an OmniSwitch NE

This procedure describes how to create a new Ethernet Ring Element or configure an existing Ethernet Ring Element on an eligible OmniSwitch NE. 6.4.4 or 7.2.1 NEs support G.8032v1. 6.4.5 R02 and 7.3.1 NEs support G.8032v2.



Note 1 — For ERP created with stacked VLAN services, only NNIs can be added as ERP path endpoints.

Note 2 — Before creating ERP with stacked VLAN services, the port/LAG mode must be Network and Bind type must be ERP, associated with that particular VLAN. To achieve this:

- From the Equipment view, chose a port. Right- click on the port, and choose Properties. The Physical Port form opens.
- Choose the Network value for the Mode parameter.
- Choose the ERP value for the Bind Type parameter.
- Port → L2 Network Interfaces → VLAN, delete the VLAN association in which the ERP needs to be created
- Port → L2 Network Interfaces → VLAN, add it to the stacked VLAN with the Bind Type value as ERP.

For 6.4.5 R02 NEs, Network port/LAG can be added in ERP without binding.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels search form opens.

2 If you are configuring an existing Ethernet Ring Element, go to step 8.

3 Click on the Create button.

4 Click on Ethernet Ring Element from the contextual menu.

5 Choose an OmniSwitch site from the Select Network Elements form to create an Ethernet Ring Element.

6 Click on the OK button. The Ethernet Ring Element (Create) form opens with the General tab displayed.

7 Go to step 10.

8 Select Ethernet Ring Element (Ethernet Ring) on the drop-down menu in the Manage Service Tunnels form. Click on the Search button to display a list of the existing ring elements.

9 Select the ring element you want to configure and click on the Properties button. The Ethernet Ring Element (Edit) form opens with the General tab displayed.

10 Configure the following parameters:

- ID
- Auto-Assign ID
- Site ID
- Description
- Administrative State
- Guard Time (centiseconds)
- Revert Time (minutes)
- Ring Protection Link Type
- Name
- Service ID
- AIS Meg Level
- Virtual Channel
- Revertive Mode

The ID and Site ID are only configurable when you are creating a new Ethernet Ring Element.

11 Click on the Path Endpoints tab.

12 Perform one of the following:

a If you are configuring an existing Ethernet Ring Path Endpoint, select the required path endpoint from the list and click Properties. The Ethernet Ring Path Endpoint (Edit) form opens with the General tab displayed.

b If you are configuring a new Ethernet Ring Path Endpoint, click on the Create button. The Ethernet Ring Path Endpoint (Create) form opens with the General tab displayed.

13 Configure the following parameters for each Path Endpoint.

- Path ID
- Description
- Path Endpoint Type

The Path ID parameter is only configurable when you are creating a new Ethernet Ring Path Endpoint.

14 If you are configuring an existing Ethernet Ring Path Endpoint, go to step 22.

15 Click on the Port tab.

16 Click on the Select button. The Select Member Port form opens.

17 Click on the Search button to list the available ports. Choose the port to use for the Ethernet ring path endpoint.

18 Click on the OK button. The Ethernet Ring Path Endpoint (Create) form displays the selected member port.



Note 1 — You must select a ring element for each site that will be part of the Ethernet ring.

Note 2 — The Ethernet ring can only have one element configured as an RPL owner or None. This is configured using the element's Ring Protection Link Type parameter.

Note 3 — The Ethernet Ring Path can be a LAG or port.

Note 4 — For 6.4.5 R02 NEs, ports must be added as a tagged access interface to the corresponding VLAN before being selected as a member port for the ERP.

19 Configure the Path ID parameter.

20 Click on the OK button. The Ethernet Ring Path Endpoint (Create) form closes.

The Path Endpoints tab displays the new Ethernet Ring Path Endpoint in the list.

21 Repeat steps 3 to 20 for the other Ethernet Ring Path Endpoint you need to create, if required.



Note — If only one Ethernet Ring Path Endpoint is created, the Ethernet Ring Element will be created as a sub-ring.

22 Click OK. A dialog box appears.

23 Click Yes to close the Ethernet Ring Element form.

24 Perform one of the following:

a If you are configuring an Ethernet Ring Element on an Omniswith NE that supports G.8032v1, continue to step 25.

b If you are configuring an Ethernet Ring Element on an Omniswith NE that supports G.8032v2, go to step 28.

25 Click on the Protected Services tab to view and specify the services for the Ethernet path. The services that you add to the list (or that already appear there) are in the order of proceeding from Endpoint A to Endpoint B. Perform the following to add a standard or stacked VLAN service:



Note — Protected Services are not applicable for 6.4.5 R02 NEs.

i Click on the Add button. The Select Service form opens.

ii Click on the Search button to display a list of services available to include in this path. Only standard and stacked VLAN services can be included.

iii Select the required service and click on the OK button.

The Select Service form closes and the service you chose is displayed in the list on the Services tab.



Note 1 — 5620 SAM does not perform a validation to confirm whether the selected service is actually along the path between the two path endpoints.

Note 2 — If ERP is created with standard VLAN service, then standard VLAN services for Release 6.4.4/6.6.2 NEs and IPM Enterprise VLAN services for Release 6.6.2 NEs can be added as Protected services.

Note 3 — If ERP is created with stacked VLAN service, then stacked/IPM stacked VLAN services for 6.4.4/6.6.2 NEs can be added as Protected Services.

26 To edit or view Protected Services, click on the Properties button of a selected standard VLAN service. The Ethernet Ring Element (Edit) form opens with the General tab displayed.

27 Click on the Protected Services tab. Choose a service. The Protected Services (Edit) form opens. Click on the Properties tab to edit or view the Protected service.

28 To view collected statistics, click on the Statistics tab. To collect statistics, click on the Collect button. See “Statistics collection overview” in the *5620 SAM Statistics Management Guide* for general information about configuring and collecting statistics.

29 Click on the OK button. The Ethernet Ring Element (Edit) form closes.

Procedure 27-8 To create an Ethernet (G.8032) ring

This procedure describes how to create an Ethernet (G.8032) ring and its associate Control Service and Data service and how to assign ring elements to the ring.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels search form opens.

2 Click on the Create button.

3 Click on Ethernet Ring from the contextual menu. The Ethernet Ring (Create) form opens.

4 Configure the following parameters:

- Mgr ID
- Auto-Assign ID
- Element ID
- Name
- Description
- Hold Time Down
- Hold Time Up (deciseconds)
- Revert Time (seconds)
- Guard Time (deciseconds)
- Compatible Version
- Auto Create Global MEG
- Maintenance Domain ID
- CCM Interval
- Run CCM On Create



Note 1 — If you enable the Auto Create Global MEG parameter, the ETH-CFM tab will display all associated Global MEGs created for this Ethernet Ring.

Note 2 — If path discovery generates Ethernet Ring paths, then the Auto Create Global MEG, Maintenance Domain ID, CCM Interval, and Run CCM on Create parameters are not propagated to the per-path CFM Continuity Check tab configuration. Auto-generation of a MEG and/or MEPs can be configured on a per-path basis.

Alternatively, if path discovery is not operational (that is, no Ethernet Ring paths are populated into the Ethernet Ring), then the General tab Path CFM Defaults parameters are propagated and a MEG and/or MEPs are generated upon manual creation of the Ethernet Ring paths.

5 Click on the Apply button. The Ethernet Ring (Edit) form opens with the General tab displayed.

6 Click on the Components tab.

7 Right click on Ring Elements and choose one of the following items from the contextual menu.

a Create Ethernet Ring Element.

i Perform steps 5 to 22 in Procedure 27-6 to create an Ethernet Ring Element. When you are done, the element will be displayed on the Components tab in Ethernet Ring form.



Note 1 — You must create a ring element for each site that will be part of the Ethernet ring.

Note 2 — The Ethernet ring can only have one element configured as an RPL owner and one element configured as an RPL neighbor. This is configured using the element's Ring Protection Link Type parameter.

Note 3 — The parameter values specified in step 4 are initially populated in the Ethernet Ring Element form when creating a ring element from the Components tab. However, you can change these as required.

ii Repeat step i to create the other required ring elements.



Note — You can create all the ring elements required for the ring in one step. See step 5 in Procedure 27-6.

iii Go to step 8.

b Add an existing Ethernet Ring Element.

i The Select Element form opens.

ii Click on the Search button and select an element.

iii Click OK.

The element will be displayed on the Components tab in Ethernet Ring form.



Note 1 — You must select a ring element for each site that will be part of the Ethernet ring.

Note 2 — The Ethernet ring can only have one element configured as an RPL owner and one element configured as an RPL neighbor. This is configured using the element's Ring Protection Link Type parameter.

Note 3 — When you add an existing Ethernet endpoint, the parameter values specified in step 4 are not populated into the properties of that endpoint.

iv Repeat steps i to iii to select the other required ring elements.

8 To create an Ethernet Path:

i Right click on Paths and choose Create Ethernet Ring Path from the contextual menu to create a path. The Ethernet Path (Create) form opens with the General tab displayed.



Note — You must create a path for each element in the ring. Each element (site) in the ring will therefore have two endpoints (from two different paths) associated with it.

ii Configure the parameters:

- Auto-Assign ID
- ID
- Description

iii Click on the Endpoints tab to configure the endpoints for the path. Perform step iv to manually configure the parameters for endpoints A and B. Perform step v to select an available path endpoint on endpoints A and B.



Note — One and only one endpoint within the entire Ethernet ring must have its Ring Protection Link Type parameter configured as Ring Protection Link End. All other endpoints in the Ethernet ring must have this parameter set to a value of Normal.

iv Manually enter the following parameters to configure endpoints A and B.

- Path ID
- Ring Protection Link Type
- Administrative State
- R-APS Tag (Outer Encapsulation Value)
- R-APS Tag (Inner Encapsulation Value)
- Member Port



Note — Path endpoints cannot be administratively enabled if:

- the R-APS Tag or Member Port parameters are not configured
- a MEP is not configured on the path endpoint

v Choose an available path endpoint on endpoints A and B.

- Click on the Select button in the Path Endpoint section. The Select Path Endpoint form opens.
- Click on the Search button and select an available endpoint.
- Click OK. The endpoint parameters are automatically populated.

9 Click on the CFM Continuity Check tab to configure a CFM Test for the path.

10 Reconfigure the following parameters in the Global MEG Auto Creation panel, if required. The values that are initially displayed when you open this tab are the same ones you configured in step 4.

- Auto Create Global MEG
- Maintenance Domain ID
- CCM Interval
- Run CCM On Create



Note — If path discovery generates Ethernet Ring paths, then these parameters are not propagated to individual paths. Auto-generation of a MEG and/or MEPs may be configured on a per-path basis.

11 Click on the Select button. The Select CFM Test form opens. Perform one of the following:

a Click on the Search button to list the available CFM tests.

i Select the required CFM test.

ii Click OK.

The Select CFM Test form closes and the Global ID and ID parameters for the selected test appear on the CFM Continuity Check tab.

b Click on the Create button to create the required CFM test. The Global Maintenance Entity Group (Create) form opens, with the General tab displayed.



Note — The Initial CCM Interval for the CFM test you select or create must be set to 10 ms or 100 ms, otherwise the subsequent MEP creation will fail. The 7210 SAS-E, 7210 SAS-M and 7210 SAS-X do not support the 10 ms value.

Refer to Procedure 32-6 for information on creating the test.

12 Click on the Intermediate Services tab to view and specify the intermediate services for the Ethernet path. The services that you add to the list (or that already appear there) are in the order of proceeding from Endpoint A to Endpoint B. Perform the following to add an intermediate service:

i Click on the Create button. The Select Service form opens.

ii Click on the Search button to display a list of intermediate services available to include in this path. Only VLL services can be included.

iii Select the required service and click on the OK button.

The Select Service form closes and the service you chose is displayed in the list on the Intermediate Services tab.



Note — 5620 SAM does not perform a validation to confirm whether the selected service is actually along the path between the two path endpoints.

iv Repeat steps i to iii to add another intermediate service, if required.



Note 1 — If you have an intermediate service highlighted in the list and want to add another service immediately above it, click on the Insert Component button rather than the Create button. The Create button places an additional service at the bottom of the list, whereas the Insert Component button places it directly above a highlighted service.

Note 2 — You can change the ordering of intermediate services in the list by selecting a particular service and using the Move Up or Move Down buttons.

13 Perform this step if you need to create Interconnects for sub-rings. The Interconnects connect a sub-ring to the main ring.

a Right click on Interconnects and choose Create Ethernet Ring Interconnect from the contextual menu to create an interconnect. The Ethernet Ring Interconnect (Create) form opens.

b Configure the parameters:

- Auto-Assign ID
- ID
- Description

c Configure the Element A end node for the interconnect.

i In the Element A panel, click on the Select button beside the ID field and select a site from the Select Element - Ethernet Ring Interconnect form.

ii Configure the parameters:

- Type
- Interconnected Ethernet Ring Element
- Propagate Topology Change

d Configure the Element B end node for the interconnect.

i In the Element B panel, click on the Select button beside the ID field and select a site from the Select Element - Ethernet Ring Interconnect form.

ii Configure the parameters:

- Type
- Interconnected Ethernet Ring Element
- Propagate Topology Change

14 To automatically create a Control service for the Ethernet (G.8032) ring, go to step 15. To manually create the Control service, go to step 18.

15 To automatically create a Control service for the Ethernet (G.8032) Ring:

i Click on the Create Control Service button. The Create Control Service form opens.

ii Click on the Select button beside the Customer field and select a customer from the Select Customer form.

iii Configure the following parameters if your Ethernet Ring is an Ethernet Virtual link sub-rings.

- Upper Ring Outer Encap
- Upper Ring Inner Encap

iv Click on the Select button beside the Control Service Template field if required and select a template from the Select Control Service Template form.



Note 1 — Only use the Control Service Template if you need to customize the parameter fields associated with the sites or SAPs such as the description or name.

Note 2 — If you need to create a Control Service Template, choose, Manage→Templates from the 5620 SAM main menu. Click on the Browse Example button and select the Ethernet Ring example. For more information about creating service tunnel templates, see "Managing templates" in the *5620 SAM Scripts and Templates Developer Guide*.

Note 3 — If a template is not specified, all created objects will use their default property values.

v Click on the OK button to apply the changes and close the form.

16 Click OK. A dialog box appears.

17 Click Yes to close the Ethernet Ring (Create) form.

18 Manually create a Control service for the Ethernet ring if you did not auto-create one in step 15.

i Perform Procedure 68-1 to create a Control service on a VPLS.

ii Perform Procedure 68-24 to create an L2 Access Interface for each path endpoint in the Ethernet ring. Each site in the Control VPLS must have two control L2 Access Interfaces.

When creating the L2 access interfaces, ensure the following requirements:

- The Terminating Port and Encap Type must have the same values used to create the particular path endpoint in step 8.
- The Outer Encapsulation Value and Inner Encapsulation Value parameters for the port in each L2 Access Interface must be set to the same value as the R-APS Tag (Outer Encapsulation Value) and R-APS Tag (Inner Encapsulation Value) respectively that you used for the particular path endpoint in step 8. This defines the interface as a Control SAP for the Ethernet ring.

19 Perform Procedure 68-1 to create the Data services on the VPLS required for the Ethernet Ring. The Data service must be a regular VPLS, I-VPLS, or B-VPLS type.

20 To automatically connect the Data services to the Ethernet Ring, go to step 21. To manually connect the Data service, go to step 22.

21 To automatically connect the Data service to the Ethernet Ring:

i Select one or more Site icon(s) associated with the Data service and choose Connect to Ethernet Ring from the contextual menu. The Connect to Ethernet Ring form opens.



Note — When you use the Connect to Ethernet Ring function to connect a data service to an Ethernet ring configured with a transit service, the 5620 SAM creates VLAN-specific SAPs for the data service only on the ring site for which Connect to Ethernet Ring is selected. The transit SAPs on the ring transparently forward traffic through other sites on the service.

ii Click on the Select button beside the Select Ethernet Ring field and select a Ethernet ring from the Select Ethernet ring form.

iii Configure the following parameters.

- Data Service Outer Encap
- Data Service Inner Encap

iv Click on the Select button beside the Data Site Template field if required, and select a template from the Data Site Template form.



Note 1 — Only use the Data Site Template, if you need to create an I-VPLS or B-VPLS type data service.

Note 2 — If you need to create a Data Site Template, choose Manage→Templates from the 5620 SAM main menu. Click on the Browse Example button and select the Ethernet Ring example.

Note 3 — If a template is not specified, all created objects use their default property values.

v Click on the OK button to apply the changes and close the form.

22 To manually connect the Data service to the Ethernet Ring, perform Procedure 68-24 to create an L2 Access Interface for each path endpoint in the Ethernet ring. Each site in the Data service must have at least two L2 Access Interfaces.



Note — When creating the L2 access interfaces, the Terminating Port and Encap Type must have the same values used to create the particular path endpoint in step 8.

Procedure 27-9 To create an Ethernet (G.8032v2) ring on OmniSwitch NEs

This procedure describes how to create an Ethernet (G.8032v2) ring on OmniSwitch 6.4.5 R02 and 7.3.1 NEs.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels search form opens.

2 Click on the Create button.

3 Click on Ethernet Ring from the contextual menu. The Ethernet Ring (Create) form opens.

4 Configure the following parameters:

- Mgr ID
- Auto-Assign ID
- Element ID
- Name
- Description
- Service Composition

5 If the Service Composition parameter was set to VPLS or VPLS and VLAN, configure the following parameters:

- Hold Time Down (centiseconds)
- Hold Time Up (deciseconds)
- Revert Time (seconds)
- Guard Time (deciseconds)
- Compatible Version

6 If the Service Composition parameter was set to VLAN or VPLS and VLAN, perform the following steps to configure control service defaults:

i Configure the VLAN Application Type parameter.

ii Click on the Select button in the VLAN Control Service panel. A list of VLAN services is displayed.

iii Choose a service from the list and click on the OK button. The VLAN service information is displayed on the Ethernet Ring (Create) form.

7 Click on the Apply button. The Ethernet Ring (Edit) form opens with the General tab displayed.

8 Click on the Components tab.

9 Right click on Ring Elements and choose one of the following items from the contextual menu:



Note 1 — You must create a ring element for each site in the Ethernet ring, and a path for for each of these ring elements. Each element will therefore have two endpoints (from two different paths) associated with it.

Note 2 — The Ethernet ring can only have one element configured as an RPL owner and one element configured as an RPL neighbor. This is configured using the element's Ring Protection Link Type parameter.

Note 3 — The parameter values specified in step 4 are initially populated in the Ethernet Ring Element form when creating a ring element from the Components tab, however, you can change these as required.

Note 4 — One and only one endpoint within the entire Ethernet ring must have its Ring Protection Link Type parameter configured as Ring Protection Link End. All other endpoints in the Ethernet ring must have this parameter set to a value of Normal.

a Create Ethernet Ring Element with path endpoints.

i See Procedure 27-7 for information about creating an Ethernet Ring Element with path endpoints on OmniSwitch NEs. The element will be displayed on the Components tab in Ethernet Ring (Edit) form.

ii Repeat step i to create the other required ring elements with path endpoints.

b Add an existing Ethernet Ring Element.

i The Select Element form opens.

ii Click on the Search button and select an element.

iii Click OK. The element will be displayed on the Components tab in the Ethernet Ring (Edit) form.

iv Repeat steps i to iii to select the other required ring elements.

10 Right click on Paths and choose Properties from the contextual menu. The Ethernet Ring Paths (Edit) form opens.

11 Click on the CFM Continuity Check tab to configure a CFM Test for the path.

12 Configure the Auto Create Global MEG parameter.

13 Click on the Select button next to the Maintenance Domain parameter. A list of maintenance domains appears.

14 Choose a maintenance domain from the list and click on the OK button. The maintenance domain information is displayed on the Ethernet Ring Paths (Edit) form.

15 Configure the CCM Interval and Run CCM On Create parameters.

16 Click on the Select button in the CFM Test panel. The Select CFM Test form opens. Perform one of the following:

a Click on the Search button to list the available CFM tests.

i Select the required CFM test.

ii Click OK.

The Select CFM Test form closes and the Global ID and ID parameters for the selected test appear on the CFM Continuity Check tab.

b Click on the Create button to create the required CFM test. The Global Maintenance Entity Group (Create) form opens, with the General tab displayed.

Refer to Procedure 32-6 for information about creating the test.



Note — The Initial CCM Interval for the CFM test you select or create must be set to 10 ms or 100 ms, otherwise the subsequent MEP creation will fail.

17 Close the Ethernet Ring Paths (Edit) form.

18 Click Yes to close the Ethernet Ring (Create) form.

Procedure 27-10 To configure a transit service on an Ethernet ring

Perform this procedure to create a transit service on a VPLS G.8032 Ethernet ring. The Ethernet ring must already exists. See "Transit services" in section 27.3.

Transit services are supported on the 7210 SAS-D and 7210 SAS-M (in access-uplink mode), Release 4.0 R7 or later, and on the 7210 SAS-T.

Transit SAPs apply only on QinQ ports.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form opens.

2 Choose Ethernet Ring (Ethernet Ring) from the drop-down menu and click on the Search button. A list of Ethernet ring services is displayed.

3 Choose an Ethernet ring from the list and click on Properties. The Ethernet Ring (Edit) form opens with the General tab displayed.

4 Click on the Create Transit Service button. If the button is not visible, click on the More Actions button and choose Create Transit Service. The Create Transit Service form opens.

5 Click on the Select button beside the Customer field and choose a customer from the Select Customer form.

6 Configure the parameters:

- Transit Service Outer Encap
- Transit Service Inner Encap



Note — The default value for these parameters is *, or 4095. When you create a transit service, you must leave the parameters at the default value.

7 Click on the Select button beside the Transit Service Template field if required and choose a template from the Select Transit Service Template form.



Note 1 — Only use the Transit Service Template if you need to customize the parameter fields associated with the sites or SAPs such as the description or name.

Note 2 — If you need to create a Transit Service Template, choose Manage→Templates from the 5620 SAM main menu. Click on the Browse Example button and choose the Ethernet Ring example. For more information about creating service tunnel templates, see "Managing templates" in the *5620 SAM Scripts and Templates Developer Guide*.

Note 3 — If a template is not specified, all created objects use their default property values.

8 Click on the OK button. A dialog box appears.

9 Perform one of the following:

a To view the properties for the service, click on the Yes button. The properties form for the transit service opens, with the General tab displayed. View the properties, and close the form. The Ethernet Ring (Edit) form is displayed.

b Click on the No button. The Create Transit Service form closes and the Ethernet Ring (Edit) form is displayed.

10 Discover the transit service.

i Click on the Flow-through Services tab. A list of services is displayed.

ii Click on the Discover Services button. The transit service is added to the list.

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The Ethernet ring (Edit) form closes.



Note — You can combine transit services using the composite service functionality in the 5620 SAM. Composite services are created automatically when Auto Discover Composite Services is enabled in System Preferences, or manually using the Rediscover Composite Services function. See chapter 74 for more information about composite services.

Procedure 27-11 To discover service tunnels

Use this procedure to list all service tunnels objects (SDPs, Ethernet rings, Ethernet tunnels, other services, and so forth) that are currently used by the service you are querying.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services is displayed.

3 Choose a service in the list and click on the Properties button. The Service (Edit) form opens with the General tab displayed.

4 Click on the Service Tunnels tab.

5 Click the Discover Service Tunnels button to re-populate the list.

Any previously discovered service tunnels on the service are removed and an on-demand re-discovery of these is triggered.

A confirmation dialog appears when the discovery is complete.

6 Click OK.

7 Click on an item in the list and the Properties button to view the object information.

8 Close the Service (Edit) form.

Procedure 27-12 To discover flow-through services

Use this procedure to list all other services that are currently using the object you are querying as a service tunnel. These are collectively referred to as flow-through services. Refer to the "Service tunnel overview" section for a list of applicable service tunnel objects.

1 Open the configuration form of the object you want to examine.

2 Click on the Flow-through Services tab.

3 Click the Discover Flow-through Services button to re-populate the list.

Any previously discovered flow-through services are removed and a manual re-discovery of these is triggered.

A confirmation dialog appears when the discovery is complete.

4 Click OK.

5 Click on a service in the list and the Properties button to view the service information.

6 Close the object's configuration form.

Procedure 27-13 To view and manage service tunnels and tunnel elements

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form opens

2 Configure the filter criteria from the drop-down menu. The filter list contains all of the object types that can be used as service tunnels, along with related service tunnel management objects. The listing is hierarchical and includes:

- Ethernet Ring Element
- Ethernet Tunnel Endpoint
- Radio Ring
- Service Tunnel
  - Ethernet Tunnel
  - Ethernet Ring
  - P2MP LSP
  - ODU Trail
  - Service (Service Management)
    - IES Service
    - MPR VLL
    - Mirror Service
    - Optical Transport Service
    - VLAN Service
    - VLL
    - VPLS
    - VPRN
  - Tunnel (Service Tunnel Management)
- Tunnel Selection Profile



Note — For all service tunnel objects except Service, the search will display all objects of that type, regardless of whether or not they are being used as a service tunnel.

If you want to see only those objects that are currently being used as a service tunnel, enable the check box for the “Used By a Service” configurable filter item that exists in the list form.

3 Click on the Search button. A list containing the selected object type is displayed.



Note — If you searched on Service (or on a specific service type) used as a service tunnel, be aware that the generated list contents are subject to change, depending on current usage and on when the last on-demand (manual) discovery was conducted. There is no auto-discovery for this listing.

In other words, only those services will be listed that were known to be used as service tunnels when the last discovery was conducted. Because the discovery is only updated on user demand, the list of services generated here may not be up to date.

Procedure 27-11 details the on-demand discovery of service tunnels (including a service used by another service as a tunnel).

4 Choose a service tunnel in the list and click on the Properties button. The Tunnel (Edit) form opens with the General tab displayed.

5 View or configure the parameters on the General tab, as required.

6 View the States and State Cause indicators, if applicable, for troubleshooting information, such as a failed OAM diagnostic.

7 Click on the other tabs to view information or modify the parameters.

8 Save the changes and close the Tunnel (Edit) form.

9 Close the Manage Service Tunnels form.

Procedure 27-14 To view the service tunnel topology

1 Choose Application→Service Tunnel Topology from the 5620 SAM main menu. The Service Tunnel Topology map opens.

2 View the topology map as required. See chapter 6 for information about using topology maps.

3 Close the topology map.

Procedure 27-15 To run an OAM validation test on a service tunnel

An OAM validator test suite must be created for the tested entity. See chapter 77 for more information about how to create an OAM validator test suite.



Note — As an alternative, you can also run an OAM validation test on the service tunnel by performing a One Time Validation. This is a mostly automated procedure and is described in Procedure 77-9.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form opens

2 Configure the filter criteria and click on the Search button. A list of service tunnels is displayed.

3 Choose a service tunnel in the list and click on the Properties button. The Tunnel (Edit) form opens with the General tab displayed.

4 Click on the Validate button. If the Validate button is not visible, click on the More Actions button and choose Validate.

If an OAM validator test suite is not associated to the service tunnel, a dialog box appears. Perform the following steps:

i Click on the OK button to associate the service tunnel with an existing OAM validator test suite. The Choose Validator Test Suite form appears.

ii Configure the filter criteria. A list of OAM validator test suites appears.

iii Choose a OAM validator test suite and click on the OK button. The Choose Validator Test Suite form closes.

5 View the State Cause indicators. When the validation test fails, a check mark appears beside the OAM Validation Failure indicator.

6 Click on the Tests tab.

7 Click on the Tested Entity Result tab.

8 Choose an entry and click on the Properties button. The Tested Entity Result (Edit) form opens with the General tab displayed.

9 Click on the Results tab to display the validation test results.

10 If you need to compare two test results from the same type of test, choose the two test results and click on the Compare button; the Difference form opens. Otherwise, go to step 13.

11 Compare the test results.

12 Close the Difference form.

13 Close the Tested Entity Result (Edit) form.

14 Close the Tunnel (Edit) form.

15 Close the Manage Service Tunnels form.

Procedure 27-16 To perform an Ethernet (G.8032) ring audit

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form opens.

2 Configure the filters and click on the Search button. A list of Ethernet rings appears.

3 Perform one of the following:

- **a** To perform a global Ethernet ring audit, go to step 4,
- **b** To perform a local Ethernet ring audit, go to step 7.

4 Click on the Global Ring Audit button. The Global Ring Audit dialog box appears.

5 Click on the Yes button. The dialog box closes, and the Ring Audit progress window appears. When the audit completes, a notification box appears.

6 Click on the Yes button. Go to step 9.

7 Select an Ethernet ring from the list, and click on the Properties button. The Ethernet Ring (edit) form appears.

8 Click on the Ring Audit button. When the audit completes, a warning or information window appears displaying the results of the audit.

9 If the audit encountered any problems that could not be resolved, an alarm is raised against the Ethernet ring listing the problems. To clear the alarm, resolve the problems and then repeat the audit.

28 — Lawful Intercept

28.1 Lawful Intercept overview *28-2*

28.2 Workflow to configure LI *28-4*

28.3 5620 SAM LI configuration procedures *28-5*

28.1 Lawful Intercept overview

Lawful Intercept, or LI, is a term that describes the interception and monitoring of network subscriber traffic by authorized agencies for law-enforcement purposes. A subscriber whose traffic is intercepted using LI is called a target. LI target traffic is replicated by a service mirror that uses subscriber information as the match criteria. LI has the following characteristics.

- LI is not detectable by a target subscriber.
- LI-related traffic is delivered separately from other network traffic.
- LI-related alarms only appear for authorized LI users.
- LI configuration information is stored in a separate and encrypted file.
- LI uses SSL security for data encryption, server authentication and message integrity between the 5620 SAM server and the single-user GUI clients or client delegate servers.

LI functions are managed separately from other 5620 SAM functions. LI mirroring is a special type of service mirroring that requires the following:

- on each LI NE in a mirror service:
  - SSH user security
  - an LI user profile
  - a user account that has LI privileges
- on the 5620 SAM:
  - SSL on the single-user GUI clients, client delegate servers and JMS server
  - a user account that has LI privileges
  - an assigned Lawful Interception Management scope of command role
  - an LI mediation policy

LI management requires a dedicated user authorization level. The 5620 SAM LI configuration forms, parameters, mirror services, and mirrored traffic are displayed only for a user with LI privileges, who can perform the following:

- create, configure, and view LI sources that use IP, MAC, SAP, and subscriber filters
- view LI-related alarms
- configure LI mediation policies
- modify the LI user password



Caution — An LI user password cannot be modified unless it is known. When an LI user password is not known, the LI user account is unavailable.



Note — Viewing or retrieving LI user activity records requires a user account with an assigned Lawful Interception Management scope of command role. The scope is restricted to the records of users in the same LI user group.

To further enhance security, LI policies and filters, and LI-related alarms are completely hidden from users without LI privileges.

See chapter 69 for more information about mirror service management. See "5620 SAM user security tasks" in the *5620 SAM System Administrator Guide* for more information about user privileges and scope of command roles. See chapter 44 for more information about filter policy configuration.

Security

The 5620 SAM admin user, or an operator with an assigned Administrator scope of command role, must create an LI user account to be used for LI configuration. A user with the admin scope of command can perform only the following LI functions:

- Create an LI user scope of command profile and associate a non-admin user account with the LI profile.
- Configure an LI user profile that is restricts the LI user to LI activities only and does not allow system administrator activities.
- Create a password for the LI user.
- Configure CLI and SNMP access for the LI user account.

The 5620 SAM admin user cannot perform the following LI functions:

- Assign LI privileges to a user who is associated with the admin profile.
- View LI-related alarms.
- Delete an LI user.
- View, create, modify, or delete LI objects.
- View or modify LI mediation policies.

The following conditions apply to LI users and LI user groups:

- LI configuration requires the Lawful Interception Management scope of command role.
- The Lawful Interception Management role can be assigned to only one scope of command profile.
- A scope of command profile that has an assigned Lawful Interception Management role can include other roles except for the admin role.
- You cannot change the scope of command profile assignment for a user group when the profile includes the Lawful Interception Management role.
- An LI user group must be created as an LI user group; you cannot change a non-LI user group to an LI user group
- You cannot change an LI user group to a non-LI user group.
- A user account can have the Lawful Interception Management or the admin role, but not both.
- A user who belongs to an LI user group cannot be changed to a non-LI user.
- An LI span of control profile restricts LI user access to specific NEs.

28.2 Workflow to configure LI

The following is the sequence of high-level activities required to configure LI using the 5620 SAM.

1. Enable SSH security on each NE that is to perform an LI function. For more information about configuring SSH, see chapter 10.
2. Enable SSL security between the 5620 SAM main server and single-user GUI clients, and between the 5620 SAM main server and client delegate servers. For more information about configuring SSL security, see "Configuring SSL security" in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.
3. Plan the 5620 SAM LI user-account creation according to the requirements for LI user access to other 5620 SAM functional areas.
4. As the 5620 SAM admin user, perform the following steps to create an LI user on the 5620 SAM. See Procedure 28-1 for more information.
   - **i** Create a 5620 SAM LI scope of command profile that has an assigned Lawful Interception Management role.
   - **ii** Create a 5620 SAM LI user group that is associated with the new scope of command profile.
   - **iii** Create a 5620 SAM LI user account and assign it to the new user group.
   - **iv** If required, create an additional NE LI user account using the 5620 SAM GUI. See Procedure 28-2 for more information.
5. Provide the login credentials for the 5620 SAM LI user account to the authorized LI administrator or LI user.
6. As the LI user, change the password of the 5620 SAM LI user account so that it is unknown to the 5620 SAM admin user. See "5620 SAM user security tasks" in the *5620 SAM System Administrator Guide* for more information.
7. As the NE admin user, perform the following steps using a CLI to create an LI user on the NE.
   - **i** Create an LI user profile on the NE. See Procedure 28-3 for information about creating an NE user profile using a CLI.
   - **ii** Create an LI user account on the NE that is associated with the LI user profile. See Procedure 28-4 for information about creating an NE user account using a CLI.

8 Provide the login credentials for the LI NE user account to the LI user.

9 As the LI user, perform the following steps as required.

i Change the password of the LI NE user account so that it is unknown to the NE admin user. See Procedure 28-5 for more information.

ii Synchronize the global LI NE user configuration profile with the local LI NE user configuration profile. If you do not synchronize the local profile with the global profile, the LI NE user does not appear in the list of users for SNMPv3 for the LI mediation policy. See Procedure 28-6.

iii Create a LI mediation policy for the NE that uses SSH for CLI sessions and secure file transfers. See Procedure 28-7 for more information.

iv Create a Block Reservation policy to reserve a filter entry block in the base ACL MAC filter for LI MAC Filter entries. See Procedure 44-9 for more information.

v Create a LI MAC filter policy to filter out traffic to non-LI users for LI mirror services. See Procedure 44-8 for more information.

vi Specify whether the NE stores the LI source configuration locally or reconfigures the LI sources after a reboot. See chapter 69 for information about saving LI source configurations.

vii Use the 5620 SAM to enable NE discovery for LI. See Procedure 28-8 for more information.

viii Configure LI mirror services, including associating the LI MAC filter policy to the LI mirror service created in step v. See chapter 69 for information about configuring mirror services.

ix Configure the LI Filter Lock to configure who can modify base IPv4 and MAC filters referenced by an LI Source. See Procedure 28-9 for more information.

x View LI user and system logs to monitor LI activity. See “User activity logging” in the *5620 SAM System Administrator Guide* for more information about accessing user and system logs.

xi Configure LI on a specific NAT subscriber. See Procedure 28-10 for more information.

xii Enable or disable use of an SSL connection for LI users and to make HTTPS requests over the XML OSS interface and the 5620 SAM GUI. See Procedure 28-11 for more information.

28.3 5620 SAM LI configuration procedures

This section describes how to configure LI on the 5620 SAM and on an NE.

Procedure 28-1 To create an LI user account on the 5620 SAM



Note — You require 5620 SAM admin user privileges to perform this procedure.

1 Using an account with an assigned User Management scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Management (Edit) form opens with the General tab displayed.

2 Click on the Scope of Command tab.

3 Click on the Create button and choose Profile from the drop-down list. The Scope of Command Profile (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Auto-Assign ID
- Profile ID
- Profile Name
- Description

5 Assign one or more scope of command roles to the profile. Perform the following steps.

i Click on the Roles tab.

ii Click on the Add button. The Select Role - Role form opens.

iii Select one or more roles to include in the scope of command profile.



Note 1 — One of the roles you choose must be the Lawful Interception Management role.

Note 2 — You cannot include the Administrator role in an LI scope of command profile.

Note 3 — The 5620 SAM allows the creation of only one scope of command profile that contains the Lawful Interception Management role.

iv Click on the OK button. The Select Role - Role form closes and a dialog box appears.

v Click on the OK button.

vi Click on the OK button. The Scope of Command Profile (Create) form closes.

6 Click on the User Groups tab.

7 Click on the Create button. The User Group (Create) form opens with the General tab displayed.

8 Configure the parameters:

- User Group
- Description
- User Group State
- Apply Local Authentication Only
- Account Expiry
- Password Expiry
- Override Global Timeout
- Client Timeout (minutes)

9 Perform the following steps to assign the new LI scope of command profile to the user group.

i Click on the Select button beside the Profile ID field in the Scope of Command panel. The Select Scope of Command Profile - User Group form opens.

ii Select the LI scope of command profile from the list and click on the OK button. The Select Scope of Command Profile - User Group list form closes and the User Group (Create) form is refreshed with the scope of command profile information.

10 Perform the following steps to assign a span of control profile to the user group.

i Click on the Select button beside the Profile ID field in the Span of Control panel. The Select Span of Control Profile - User Group form opens.

ii Select a profile from the list and click on the OK button. The Select Span of Control Profile - User Group list form closes and the User Group (Create) form is refreshed with the span of control profile information.

11 Click on the OK button. The User Group (Create) form closes and the 5620 SAM User Security - Security Management (Edit) form reappears.

12 Click on the Users tab.

13 Click on the Create button. The User (Create) form opens.

14 Configure the parameters:

- User Name
- Description
- User State
- E-mail Address
- Password Change Required
- User Password
- Confirm Password
- Valid Client IP address
- Enable IP Address validation

15 Perform the following to associate the user with the newly created LI user group.

i Click on the Select button beside the User Group parameter. The groupName - User list form opens.

ii Choose the LI user group from the list and click on the OK button. The groupName - User list form closes and the User (Create) form is refreshed with the user group information.

16 Click on the OK button. The User (Create) form closes and the 5620 SAM User Security - Security Management (Edit) form reappears.

17 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 28-2 To create an additional NE LI user account using the 5620 SAM GUI



Note 1 — You require 5620 SAM LI user privileges to perform this procedure.

Note 2 — Before you can perform this procedure, at least one LI user account must exist on the NE.

Note 3 — Before you can perform this procedure, a 5620 SAM LI user must enable LI discovery for the NE using Procedure 28-8.

1 Choose Administration→Security→NE User Configuration from the 5620 SAM main menu. The NE User Configuration form opens.

2 Click on the Create button. The NE User (Create) form opens with the General tab displayed.

3 Configure the following parameters:

- User Name
- Description
- Access

You must specify the li, snmp, and console values for the Access parameter.

Additional configurable parameters are displayed.

4 Configure the additional parameters:

- Password
- Confirm Password
- Home Directory
- Restrict to Home
- Console Login Exec File
- Console Cannot Change Password
- Console New Password At Login

Specify an MD5 authentication key for the Password parameter. See Procedure 28-5 for information about generating a user authentication key.

5 Perform the following steps to assign a console profile, if required.

i Click on the Console Profiles tab. The list of profiles numbered one through eight appears. A user can have up to eight console profiles.

ii Use the Select button beside one of the Profile 1 through Profile 8 parameters to choose a console profile. See “To configure a user account for access to a managed device” in the *5620 SAM System Administrator Guide* for information about creating console profiles.

6 Click on the SNMPv3 tab.

i Enable the Authentication Protocol parameter.

ii Specify an authentication key generated using Procedure 28-5 for the New Authentication Password and Confirm New Auth Password parameters.

iii Enable the Privacy Protocol parameter.

iv Specify a DES encryption key generated using Procedure 28-5 for the New Privacy Password and Confirm New Privacy Password parameters.

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The NE User (Create) form closes and the NE User Configuration form reappears.

7 Close the NE User Configuration form.

Procedure 28-3 To create an NE LI user profile using CLI



Note — You require NE admin user privileges to perform this procedure.

1 Open an SSH session on the NE as described in chapter 11.

2 Enter the following commands in sequence at the prompt to create an NE user profile. The following is a sample configuration:

```
configure system security profile li-prof ↵
default-action deny-all ↵
li ↵
 entry 10 ↵
 match "configure li" ↵
 action permit ↵
 exit ↵
 entry 20 ↵
 match "exit" ↵
 action permit ↵
 exit ↵
 entry 30 ↵
 match "help" ↵
 action permit ↵
 exit ↵
 entry 40 ↵
 match "back" ↵
 action permit ↵
 exit ↵
 entry 50 ↵
```

```
match "show li" ↵
action permit ↵
exit ↵
entry 60 ↵
match "info" ↵
action permit ↵
exit ↵
entry 70 ↵
match "configure system security user" ↵
action permit ↵
exit ↵
entry 80 ↵
match "admin save" ↵
action permit ↵
exit ↵
exit all ↵
admin save ↵
```

3 Close the SSH session.

4 Right-click on the NE in the 5620 SAM topology map and choose Resync→Resync All MIBs from the contextual menu to update the NE configuration in the 5620 SAM.

Procedure 28-4 To create an LI user account on an NE using a CLI



Note — You require NE admin user privileges to perform this procedure.

1 Open an SSH session on the NE as described in chapter 11.

2 Enter the following commands in sequence at the prompt to create an LI user:

```
configure system security snmp ↵
```

To specify the SNMP access group configuration, perform one of the following:

a For an NE at Release 8.0 R7 or earlier, type the following:

```
access group LI_group security-model usm security-level
privacy context li exact read li-view write li-view notify iso
↵
```

b For an NE at Release 8.0 R7. 8.0 R8, 8.0 R9, 9.0 R1, or 9.0 R2, type the following:

```
access group LI_group security-model usm security-level
privacy context li exact read iso write iso notify iso ↵
```

c For a Release 8.0 NE at R10 or later, and for a Release 9.0 R3 or later NE, type the following:

```
access group "LI_group" security-model usm security-level
privacy read "iso" write "iso" notify "iso" ↵

access group "LI_group" security-model usm security-level
privacy context "li" exact read "li-view" write "li-view"
notify "iso" ↵

exit all ↵

configure system security user LI_username ↵

password LI_password ↵

snmp group LI_group ↵

console member LI_profile ↵

console no member default ↵

exit all ↵

admin save ↵
```

where
LI_group is the name of the LI user group on the NE
LI_usename is the name of the LI user account on the NE
LI_password is the password for the LI user account on the NE
LI_profile is the name of an LI user profile; see Procedure 28-3 for information about creating an LI user profile

3 Close the SSH session.

4 Right-click on the NE in the 5620 SAM topology map and choose Resync→Resync All MIBs from the contextual menu to update the NE configuration in the 5620 SAM.

Procedure 28-5 To configure NE LI user security

Perform this procedure to change the password for an LI user account on an NE and to configure LI user authentication and SNMP data encryption on the NE.



Note — You require NE LI user privileges to perform this procedure.

1 Use the NE LI user account to open an SSH session on the NE. See chapter 11 for information about opening an SSH session on an NE.

2 Enter the following command to obtain the SNMP engine ID of the NE.

```
show system info ↵
```

The SNMP engine ID is displayed.

3 Record the SNMP engine ID for use in the following steps.

4 Log in to a 5620 SAM main server, client delegate server, or single-user client station using an appropriate user account.



Note 1 — If you are logging on to a main server or client delegate server station, you must log in as the samadmin user.

Note 2 — If you are logging on to a 5620 SAM single-user client station, you must log in as a local administrator, or as the user who installed the client.

5 Open a console window.

6 Navigate to the *install_dir*/nms/bin directory

where *install_dir* is the 5620 SAM installation location, typically /opt/5620sam/server or /opt/5620sam/client on RHEL and Solaris, and C:\5620sam\client on Windows

7 Perform the following steps to generate an MD5 authentication key for the NE LI user account. An authentication key is used to create an encrypted authentication password.

i Perform one of the following.

- On a RHEL or Solaris station, enter the following at the CLI prompt:

```
./nmsclient.bash password2key MD5 password engine_ID ↵
```

- On a Windows station, enter the following at the CLI prompt:

```
nmsclient.bat password2key MD5 password engine_ID ↵
```

where
password is the ASCII password string used to generate the key
engine_ID is the SNMP engine ID obtained in step 2

The utility generates the authentication key.

ii Record the key value for use later in the procedure.

8 Perform the following steps to generate an MD5 DES privacy key for the NE LI user account. A DES privacy key is used to encrypt the SNMP packets for additional security.

i Perform one of the following.

- On a RHEL or Solaris station, enter the following at the CLI prompt:

```
./nmsclient.bash password2key MD5 password engine_ID ↵
```

- On a Windows station, enter the following at the CLI prompt:

```
nmsclient.bat password2key MD5 password engine_ID ↵
```

where
password is the ASCII password string used to generate the key
engine_ID is the SNMP engine ID obtained in step 2

The utility generates the DES privacy key.

ii Record the key value for use later in the procedure.

9 Close the console window.

10 Enter the following commands in sequence at the CLI prompt to change the LI user password and to configure LI security for the user account:

```
configure system security user username ↵

password new_LI_password ↵

snmp ↵

authentication md5 authentication_key privacy des-key
DES_privacy_key ↵

exit all ↵

admin save ↵
```

where
LI_group is the name of the LI user group on the NE
LI_username is the name of the LI user account on the NE
new_LI_password is the new password for the LI user account on the NE
authentication_key is the MD5 authentication key value generated for the NE LI user in step 7
DES_privacy_key is the DES privacy key value generated for the NE LI user in step 8

11 Close the SSH session.

Procedure 28-6 To synchronize the global 5620 SAM NE user configuration profile with the local NE user configuration profile

Perform this procedure to synchronize the global NE user configuration with the local NE user configuration. You must perform this procedure before you can create an LI mediation policy.



Note 1 — You require 5620 SAM LI user privileges to perform this procedure.

Note 2 — If you do not synchronize the local profile with the global profile, the LI NE user does not appear in the list of users for SNMPv3 for the LI mediation policy.

1 Choose Administration→Security→NE User Configuration from the 5620 SAM main menu. The NE User Configuration form opens with a list of NE users.

2 Choose the NE LI user you created in Procedure 28-4 and click on the Synchronize button. The Synchronize - SR Local User form opens.

3 Choose the NE on which the local policy is defined from the Available Nodes panel and click on the right-arrow to move the NE to the Selected Node panel.

4 Click on the Synchronize button.

5 Close the Synchronize -SR Local User form.

6 Close the NE User Configuration form.

Procedure 28-7 To configure an LI mediation policy

Perform this procedure to create an LI mediation policy that enables the creation of source objects for an LI service mirror.



Note — You require 5620 SAM LI user privileges to perform this procedure.

1 Choose Administration→Mediation from the 5620 SAM main menu. The Mediation (Edit) form opens with the General tab displayed.

2 Click on the LI Mediation Security tab.

3 Click on the Create button. The LI Mediation Policy (Create) form opens.

4 Click on the Select button beside the User Name parameter in the SNMPv3 panel to view a list of configured users. The Select User - LI Mediation Policy form opens.

5 Select the NE LI user you created in Procedure 28-4 from the list and click on the OK button. The user name is displayed on the LI Mediation Policy (Create) form.

6 The SNMP passwords in the 5620 SAM mediation policy must match the encrypted passwords generated for the NE LI user in Procedure 28-5. Perform the following steps to set the mediation-policy passwords.

   i Click on the Properties button. The NE User Configuration form opens.

   ii Click on the SNMPv3 tab.

   iii Enable the Authentication Protocol parameter.

   iv Specify the password used to generate the authentication key in Procedure 28-5 for the New Authentication Password and Confirm New Auth Password parameters.

   v Enable the Privacy Protocol parameter.

   vi Specify the password used to generate the DES encryption key in Procedure 28-5 for the New Privacy Password and Confirm New Privacy Password parameters.

   vii Click on the OK button. A dialog box appears.

   viii Click on the Yes button. The NE User Configuration form closes.

7 Click on the OK button. A dialog box appears.

8 Click on the OK button. The Mediation Policy (Create) form closes and the Mediation (Edit) form reappears.

9 Click on the OK button. The Mediation (Edit) form closes.

Procedure 28-8 To enable NE discovery for LI

Perform this procedure to enable LI discovery of an NE. Before you can enable LI discovery for an NE, the NE must be successfully discovered. See chapter 10 for information about configuring NE discovery.



Note — You require 5620 SAM LI user privileges to perform this procedure.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form opens with the Discovery Rules tab displayed.

2 Click on the Managed State tab. A list of discovered NEs is displayed.

3 Choose an NE on which Procedures 28-3 and 28-4 have been performed, and click on the Properties button. The Node Discovery Control (Edit) form opens with the General tab displayed.

4 Click on the LI Mediation Security tab.

5 Click on the Select button in the Dual Read Access Mediation Policy panel. The Configure Mediation Security - Node Discovery Control list form opens.

6 Choose the LI mediation policy created in Procedure 28-7 and click on the OK button. The Configure Mediation Security - Node Discovery Control list form closes.

7 Click on the Select button in the Dual Write Access Mediation Policy panel. The Configure Mediation Security - Node Discovery Control list form opens.

8 Choose the LI mediation policy created in Procedure 28-7 and click on the OK button. The Configure Mediation Security - Node Discovery Control list form closes.

9 Click on the Select button in the Dual Trap Access Mediation Policy panel. The Configure Mediation Security - Node Discovery Control list form opens.

10 Choose the LI mediation policy created in Procedure 28-7 and click on the OK button. The Configure Mediation Security - Node Discovery Control list form closes.

11 Click on the OK button. The Node Discovery Control (Edit) form closes and the Discovery Manager (Edit) form reappears.

12 Click on the Resync Status tab.

13 Click on the Search button. A list of NEs is displayed.

14 Choose the NE and click on the Resync button. The Resync Options form opens.

15 Select Choose MIB Entries and click on the Next button. The Choose MIB Entries list form opens.

16 Select all TIMETRA-MIRROR-MIB entries in the list and click on the Finish button.



Note — Resynchronizing only the TIMETRA-MIRROR-MIB entries resynchronizes only LI source objects and keeps the resynchronization time to the minimum required.

17 Click on the Close button. The Resync Options form closes and the Discovery Manager (Edit) form reappears.

18 Click on the OK button. The Discovery Manager (Edit) form closes.

Procedure 28-9 To configure the LI Filter Lock

This procedure allows a 5620 SAM LI user to configure a parameter that permits base IPv4 and MAC filters referenced by an LI Source to be modified or deleted. The LI Filter Lock parameter specifies who can modify the LI filters. The available options are:

- Locked: no user can modify the LI filters
- Unlocked For LI Users: only users with LI privileges can modify the LI filters
- Unlocked For All: all users can modify the LI filters



Note — You require 5620 SAM LI user privileges to view the LI Configuration Status tab and to perform this procedure.

1 Right-click on a discovered device in the Equipment navigation tree and choose Properties from the contextual menu. The Network Element (Edit) form is displayed.

2 Click on the LI Configuration Status tab.

3 Configure the LI Filter Lock parameter.

4 Click OK to apply the configuration and close the Network Element (Edit) form.

Procedure 28-10 To configure LI on a specific NAT subscriber

Perform this procedure if you need to configure LI on a specific NAT subscriber.

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria, if required, and click on the Search button. A list of mirror services appears.

3 Choose a mirror service and click on the Properties button. The Mirror *Service Name* (Edit) form opens with the General tab displayed.

4 Click on the Sites tab. A list of mirror service sites are displayed.

5 Choose a site and click on the Properties button. The Mirror Site (Edit) form opens with the General tab displayed.

6 Click on the LI NAT Sources tab.



Note — The LI NAT Sources tab appears only if the Encapsulation Type parameter for the mirror site is set to Ethernet and the L3 encapsulation Header Type parameter is set to IP-UDP Shim. See Procedure 69-3 for more information about how to configure L3 encapsulation.

7 Click on the Configure LI Source Configuration button.

8 Click on the Ethernet Header tab.

9 Configure the parameters:

- Source MAC Address
- Destination MAC Address
- EtherType

10 Click on the L2 Aware Subscribers tab.

11 Click on the Create button. The LI Source NAT L2 Aware Subscriber (Create) form opens.

12 Configure the parameters:

- Subscriber ID
- Intercept ID
- Session ID

13 Click on the OK button. A dialog box appears.

14 Click on the OK button. The LI Source NAT L2 Aware Subscriber (Create) form becomes a tab.

15 Click on the OK button. The LI Source NAT L2 Aware Subscriber (Create) tab closes and the Mirror Service (Edit) form reappears with the Sites tab displayed.

16 Choose a site and click on the Properties button. The Mirror Site (Edit) form opens with the General tab displayed.

17 Click on the LI NAT Sources tab. The Ethernet Header tab is displayed.

18 Click on the Dual Stack Lite LSN Subscribers tab.

19 Click on the Create button. The LI Source Dual Stack Lite LSN Subscriber (Create) form opens.

20 Configure the parameters:

- Routing Instance ID
- IP Address
- Prefix Length
- Intercept ID
- Session ID

21 Click on the OK button. A dialog box appears.

22 Click on the OK button. The LI Source Dual Stack Lite LSN Subscriber (Create) form becomes a tab.

23 Click on the OK button. The LI Source Dual Stack Lite LSN Subscriber (Create) tab closes and the Mirror Service (Edit) form reappears with the Sites tab displayed.

24 Choose a site and click on the Properties button. The Mirror Site (Edit) form opens with the General tab displayed.

25 Click on the LI NAT Sources tab. The Ethernet Header tab is displayed.

26 Click on the Classic LSN Subscribers tab.

27 Click on the Create button. The LI Source Classic LSN Subscriber (Create) form opens.

28 Configure the parameters:

- Routing Instance ID
- IP Address
- Prefix Length
- Intercept ID
- Session ID

29 Click on the OK button. A dialog box appears.

30 Click on the OK button. The LI Source Classic LSN Subscriber (Create) form becomes a tab.

31 Click on the OK button. The LI Source Classic LSN Subscriber (Create) tab closes and the Mirror Service (Edit) form reappears with the Sites tab displayed.

32 Click on the Apply button. A dialog box appears.

33 Click on the Yes button.

34 Close the Mirror Service (Edit) form.

35 Close the Manage Mirror Services form.

Procedure 28-11 To enable or disable the use of a secure channel for LI users

Perform this procedure to enable or disable SSL for LI users.



Caution — Contact your Alcatel-Lucent technical support representative before you attempt to modify the nms-server.xml file. Modifying the nms-server.xml file can have serious consequences that can include service disruption.



Note — You must perform this procedure on each main server in a redundant 5620 SAM deployment.

1 Log in to the 5620 SAM main server station as the samadmin user.

2 Navigate to the 5620 SAM server configuration directory, typically /opt/5620sam/server/nms/config.

3 Create a backup copy of the nms-server.xml file.

4 Open the nms-server.xml file using a plain-text editor.

5 Search for the following XML tag.

```
<liConf
```

liUserRequireSSL="value"

where *value* is set to true or false to enable or disable the secure channel check for LI users.

6 Edit the “liUserRequireSSL=” line to enable or disable SSL, as required.

7 Save and close the nms-server.xml file.

8 Open a console window.

9 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

10 If the main server is a standalone server, or the primary server in a redundant deployment, enter the following:

```
bash$ ./nmsserver.bash read_config ↵
```

The main server reads the nms-server.xml file and puts the configuration change into effect.

11 If the main server is the standby server in a redundant deployment, enter the following:

```
bash$ ./nmsserver.bash force_restart ↵
```

The main server restarts and puts the configuration change into effect.

29 — IPsec

29.1 IPsec overview ***29-2***

29.2 IPsec VPN ***29-4***

29.3 Multi-chassis IPsec ***29-7***

29.4 Sample video wholesale IPsec configuration ***29-7***

29.5 Workflow to configure and manage an IPsec configuration ***29-8***

29.6 Workflow to configure and manage an IPsec configuration using the IPsec VPN ***29-9***

29.7 Workflow to enable BFD over a static LAN-to-LAN IPsec tunnel ***29-9***

29.8 General IPsec procedures ***29-10***

29.9 IPsec VPN procedures ***29-27***

29.1 IPsec overview

The 5620 SAM supports the configuration of IPsec VPRN services, which are generically called IPsec VPNs. An IPsec VPN enables the secure extension of a corporate VPN over uncontrolled or untrusted private and public networks. The ISA tunnel on the 7750 SR, 7750 MG, and the 7450 ESS in mixed mode, provides IPsec tunneling and encryption between sites.

You can use the 5620 SAM to configure IPsec sessions and the security associations that are required in a bidirectional IPsec tunnel. You can configure multiple IPsec tunnels for a VPRN.

5620 SAM IPsec session configuration supports the following:

- encryption methods such as DES, 3DES, AES-128, AES-192, and AES-256
- authentication and hashing methods such as HMAC-MD5, HMAC-SHA1, and HMAC-SHA2
- key distribution methods such as IKE shared secret with PFS, and manual exchange
- key generation algorithms such as Diffie-Helman
- IPsec modes
- shared secret authentication
- NAT traversal for IKEv1 and IKEv2
- DPD for the IPsec tunnel

An IPsec VPN service includes IPsec tunnels that terminate on IES or VPRN IPsec gateways. These gateways support L3 forwarding through an interface that connects to an IPsec tunnel. You can use the 5620 SAM to configure VPRN services to which individual hosts connect over the Internet to an IES or VPRN IPsec gateway. You can configure one or more tunnel interfaces in a VPRN service, and can configure multiple tunnel security profiles for each tunnel interface.

IKE policies are used to negotiate IPsec security associations, or SAs, between IPsec peers. An SA is a relationship between two or more IPsec peers that defines how the peers communicate securely. IKE policies are exchanged between IPsec peers to negotiate a secure communication channel; they specify how traffic is encrypted between source and destination sites in an IPsec VPN by establishing a shared security policy using authentication keys.

IPsec transform policies specify the protocol for the IPsec authentication header and the encryption protocol for the encapsulating security payload, or ESP, and define the attributes that are used to secure the data.

After an IPsec peer initiates an IPsec session, there are two main phases:

- authentication and protection of IPsec peer identities and negotiation of matching IKE SA policies between peers to establish a secure channel for negotiating IPsec SAs in the next phase
- IPsec SA parameter negotiation and establishment of matching peer SAs

After the second phase, the IPsec peers exchange data over the IPsec tunnel according to the IPsec parameters in the IKE and IPsec transform policies.

You can create a tunnel template to configure shared IPsec transforms and IKE policies. Each IPsec peer configuration can include the following:

- one or more configured IPsec transforms
- one IKE policy
- one unique IPsec tunnel
- one tunnel filter defined in the IPsec tunnel configuration

Each IPsec tunnel between IKE peers is identified by a unique remote peer IP address or a unique local IP address.

You can use the IPsec Application Function Manager to create and manage end-to-end IPsec components to form a secure VPN. See section 29.2 for more information.

The 5620 SAM OSSI supports IPsec VPN configuration.

IPv6 IPsec

OSPFv3 authentication requires IPv6. IPv6 IPsec requires the following:

- IPsec transport mode —required because the NE acts as an OSPFv3 authentication host
- IPsec static security association—defines the SPI values, algorithms, protocol and keys to be used, and requires the same configuration at each end of the tunnel
- AH and ESP
- MD5, SHA1, and SHA2

BFD

You can use BFD for static LAN-to-LAN IPsec tunnels on the 7750 SR-c4, 7750 SR-7, 7750 SR-12, 7750 SR-12E, 7750 SR-c12, and 7450 ESS in mixed mode. The following is the configuration information for implementing BFD over static LAN-to-LAN IPsec tunnels:

- You can have only one BFD session between a source/destination address pair.
- Each tunnel can be associated with only one BFD session. However, one or more tunnels, to a maximum of 500, can be associated with same BFD session.
- If one BFD session is associated with multiple tunnels, the tunnel that carries the BFD traffic must be operationally up before any of the other tunnels can be operationally up.
- When the 5620 SAM does not receive BFD packets from a peer before the detection time expires or a signal down notification is sent from a remote peer, the BFD session is considered down. When the 5620 SAM sets the associated IPsec tunnels in a down state, 5620 SAM performs the following:
  - sends a Delete Payload message to each remote peer from each associated tunnel and SA
  - removes the state and table entries from each associated tunnel and SA

29.2 IPsec VPN

You can create and manage the association between IPsec components, public and private services, to form a secure VPN. See "Typical applications for IPsec corporate services" in this section for the typical applications of an IPsec VPN.

You use the IPsec VPN step forms to perform the following:

- Configure the corporate service type.
- Enable the link between the corporate and secure service.
- Choose an NE service site.
- Configure the secure VPRN service.
- Configure the delivery service.
- Choose the Tunnel group.
- Create the policy.
- Deploy the IPsec VPN.

Tunnel types

Table 29-1 lists the tunnel types that you can create for an IPsec VPN.

Table 29-1 Tunnel types

Tunnel type	7750 SR	7750 MG	7450 ESS in mixed mode	7210 SAS
Dynamic (site-to-site)	✓	✓	✓	
Dynamic (soft client)	✓	✓	✓	
Static	✓	✓	✓	✓

The 5620 SAM creates the following after the successful creation of an IPsec VPN, regardless of the tunnel type:

- a secure VPRN service and NE sites
- the IES or VPRN delivery service and NE sites
- if you specify that the secure and corporate services are to be linked, a composite service that contains the corporate and secure services

The 5620 SAM performs specific configuration actions after the successful creation of an IPsec VPN, depending on the tunnel type. See Procedures 29-15 to 29-17 for more information.

Typical applications for IPsec corporate services

Figure 29-1 shows one public L3 VPRN service that is associated with the corresponding private VPRN service. The private VPRN service belongs to a larger private VPRN. The public service can be a VPRN or IES service. The private service can only be a VPRN service.

Figure 29-1 Static IPsec tunnel

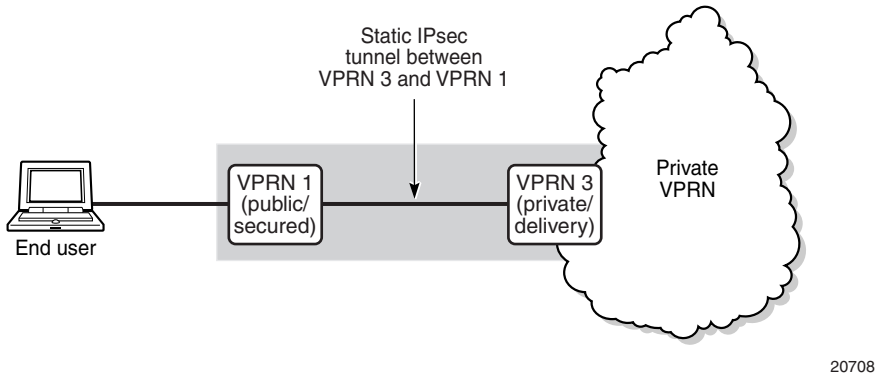


Figure 29-2 shows two public L3 VPRNs, VPRN 1 and VPRN 2, which are connected to the private, secure service VPRN 3 through an IPsec gateway. The public services can be VPRN or IES services. The private service can only be a VPRN service.

Figure 29-2 IPsec tunnels for a site

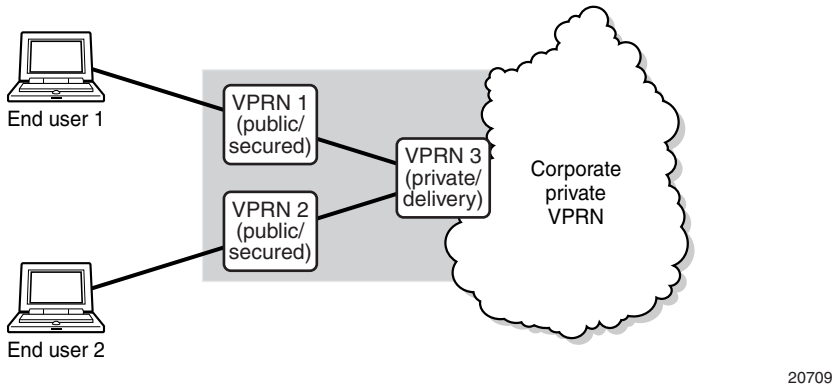


Figure 29-3 is the same as Figure 29-1, but Figure 29-3 shows IPsec tunnels across multiple sites. Site A, Site B, and Site C are part of the private service VPRN 4. For the site, there is a secure IPsec tunnel between a public service and a private service. The public services can be L3 VPRN or L3 IES services. The private service can only be a VPRN service.

Figure 29-3 IPsec tunnels for multiple sites

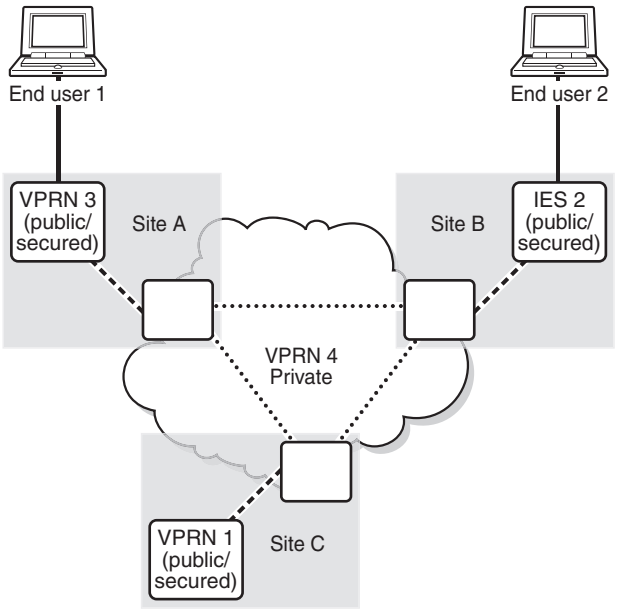
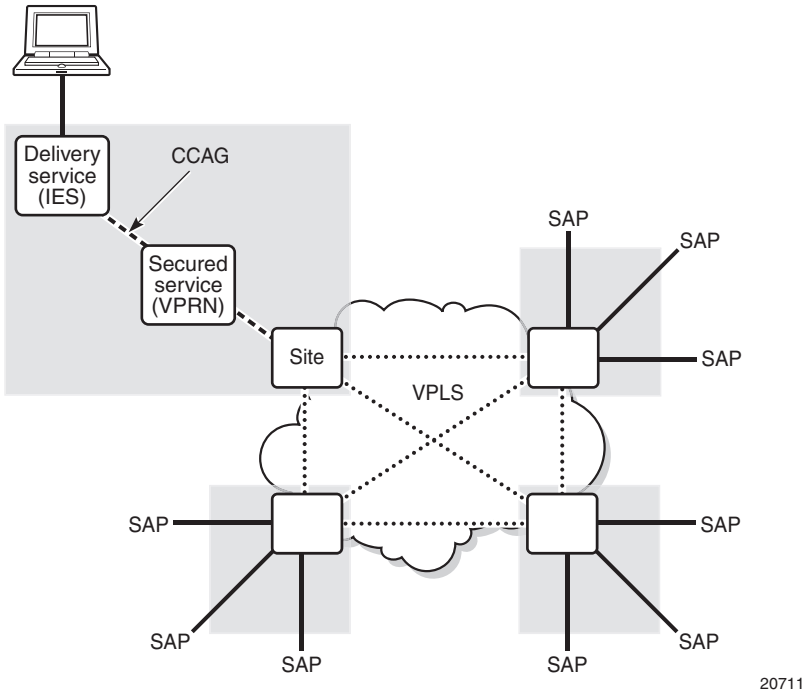


Figure 29-4 shows a private VPRN that is connected to a corporate network and a VPLS that is the corporate network. The public IES and private VPRN service are connected to VPLS network through a CCAG or SCP. CCAG connects the private VPRN to the VPLS network.

Figure 29-4 IPsec VPN in a corporate network



29.3 Multi-chassis IPsec

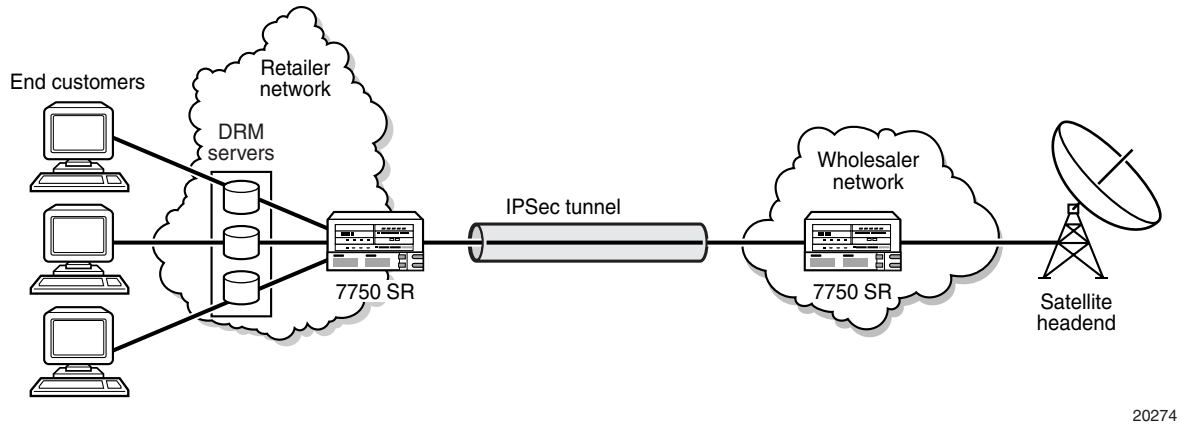
MC IPsec provides a stateful failover mechanism for IPsec tunnels between two 7750 SRs or 7450 ESSs in mixed mode—an active NE and a standby NE. Stateful failover enables IPsec traffic to continue being forwarded without interruption in the event of a failure. MC IPsec provides protection for NE failure or MS-ISA failure. When an active NE fails, the IPsec tunnels failover to the standby peer without having to re-establish the session. The failover mechanism can occur at the tunnel group level. A tunnel group can failover to the standby NE, independently of other tunnel groups on the active NE. See chapter 37.

29.4 Sample video wholesale IPsec configuration

Larger providers or a cooperative of smaller providers often unite to provide a video headend to avoid the costs of investing in a satellite headend locations on their own ground station, to provide tripleplay features. Each retail subscriber can purchase content from this single station and receive it over IP. However, encryption is required so that the signal cannot be understood if intercepted.

Figure 29-5 shows a sample video wholesale configuration with a high-speed encrypted tunnel.

Figure 29-5 Sample video wholesale configuration



29.5 Workflow to configure and manage an IPsec configuration

See section 29.6 for the workflow to configure and manage an IPsec configuration using the IPsec VPN step forms.

1. Provision the ISA tunnel MDA on the 7750 SR, 7750 MG, or 7450 ESS in mixed mode. See chapters 12 and 13 for more information about IPsec equipment configuration.
   - **i** Create or configure ISA-tunnel groups.
   - **ii** Assign the active and backup tunnel group members to the ISA-tunnel groups.
2. Configure an IKE policy. See Procedure 29-1 for more information.
3. Configure an IPsec transform policy. See Procedure 29-2 for more information.
4. If your network will include shared IPsec transform and IKE policies, then configure an IPsec tunnel template. See Procedure 29-4 for more information.
5. Configure an IPsec security policy. See Procedure 29-5 for more information.
6. If you are configuring IPsec on a VPRN, create the private-facing tunnel interface. See Procedure 29-6 for more information.
   - **i** Create a private IPsec SAP.
   - **ii** Configure ingress and egress policies, if required.
7. Create the public-facing tunnel interface. See Procedure 29-8 for more information.
   - **i** Create an L3 access interface on an IES or VPRN. See chapters 70 and 71 for more information about creating an L3 access interface.
   - **ii** Define the IPsec public SAP for the L3 access interface.
   - **iii** Specify the IPsec gateway, if required, on the NE.

8 If you are configuring IPsec on a VPRN, then create IPsec tunnels on the VPRN tunnel interface. See Procedure 29-7 for more information.

9 Configure the static route.See Procedure 22-13 for more information.

29.6 Workflow to configure and manage an IPsec configuration using the IPsec VPN

1 Create a corporate service and, if required, a service template. See Table 29-2 and the *5620 SAM Scripts and Templates Developer Guide* for more information.

2 Create an IPsec VPN. See Procedure 29-10 for more information.

3 Select the NE service sites for the IPsec VPN. See Procedure 29-11 for more information.

4 Create or select the secure VPRN service for the IPsec VPN. See Procedure 29-12 for more information.

5 Create or select the delivery service for the IPsec VPN. See Procedure 29-13 for more information.

6 Select the tunnel group for the IPsec VPN. See Procedure 29-14 for more information.

7 Assign policies and configurations to the IPsec VPN.

a If you chose Dynamic (Site-to-Site) for the Tunnel Type parameter in step 2 of Procedure 29-14, then see Procedure 29-15 for more information.

b If you chose Dynamic (Soft Client) for the Tunnel Type parameter in step 2 of Procedure 29-14, then see Procedure 29-16 for more information.

c If you chose Static for the Tunnel Type parameter in step 2 of Procedure 29-14, then see Procedure 29-17 for more information.

8 Deploy the IPsec VPN.

29.7 Workflow to enable BFD over a static LAN-to-LAN IPsec tunnel

1 Create an tunnel interface on a VPRN, as described in Procedure 29-6.

2 Create an IPsec tunnel on the VPRN tunnel interface, as described in Procedure 29-7.

3 Enable BFD for the static LAN-to-LAN IPsec tunnel, as described in Procedure 29-9.

4 Assign a BFD service and interface that can be used for the BFD session on the IPsec tunnel.

29.8 General IPsec procedures

The following procedures describe how to perform general 5620 SAM IPsec configuration tasks, such as policy creation. See section 29.9 for IPsec VPN procedures.

Procedure 29-1 To configure an IKE policy

1 Choose Policies→ISA Policies→IKE from the 5620 SAM main menu. The IKE Policy form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy, if required, and click on the Search button. Choose a policy from the list and click on the Properties button. The IKE Policy (Edit) form opens with the General tab displayed.

b Click on the Create button. The IKE Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Auto-Assign ID
- ID
- Version
- Description
- Mode
- Diffie-Hellman (DH) Group
- Perfect Forward Secrecy (PFS)
- PFS DH Group
- Authentication Algorithm
- Authorization Method
- Encryption Algorithm
- Internet Security Association and Key Management Life Time (seconds)
- IPsec Life Time (seconds)
- Self Authorization Method

4 Click on the NAT Traversal tab.

5 Configure the parameters:

- NAT Traversal
- Keep Alive Interval
- Force Keep Alive

6 Click on the DPD tab.

7 Configure the parameters:

- Dead Peer Detection (DPD)
- Interval
- Max Retries

The Interval and Max Retries parameters are not configurable if the Dead Peer Detection (DPD) parameter is set to Disabled.

8 Click on the Apply button.

9 Click on the General tab.

10 Click on the Distribute button to manually distribute the policy locally to devices. if the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

11 Close the IKE Policy (Create) form.

12 Close the IKE Policy form.

Procedure 29-2 To configure an IPsec transform

1 Choose Policies→ISA Policies→IPSec Transform from the 5620 SAM main menu. The IPSec Transform form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy, if required, and click on the Search button. Choose a policy from the list and click on the Properties button. The IPSec Transform (Edit) form opens with the General tab displayed.

b Click on the Create button. The IPSec Transform (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Auto-Assign ID
- Policy ID
- Description
- Authentication Algorithm
- Encryption Algorithm

4 Click on the Apply button.

5 Click on the Distribute button to manually distribute the policy locally to devices. if the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

6 Close the form.

7 Close the IPSec Transform form.

Procedure 29-3 To create an IPsec static security association

1 Choose Policies→ISA Policies→IPSec Static Security Association from the 5620 SAM main menu. The IPSec Static Security Association Policies form opens.

2 Click on the Create button. The IPsec Static Security Association (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Static SA Name
- Direction
- Protocol
- Authentication Algorithm
- Authentication Key Type
- Authentication Key
- Security Parameter Index
- Static SA Description

4 Click on the Apply button.

5 Click on the Distribute button to manually distribute the policy locally to devices. if the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

6 Close the form.

7 Close the IPsec Static Security Association (Create) form.

Procedure 29-4 To create an IPsec tunnel template

1 Choose Policies→ISA Policies→IPSec Tunnel Template from the 5620 SAM main menu. The IPSec Tunnel Template Policies form opens.

2 Click on the Create button. The IPSec Tunnel Template (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Auto-Assign ID
- Policy ID
- Description
- Reverse Route
- Replay Window

4 Click on the IPSec Transforms tab.

5 Click on the Select button in the Transform ID 1 to Transform ID 4 panels. The Select Transform ID *1_4* IPSec Tunnel Template list form opens.

6 Choose an entry and click on the OK button. The Select Transform ID *1_4* IPSec Tunnel Template list form closes.

7 Click on the General tab.

8 Click on the Apply button.

9 Click on the Distribute button to manually distribute the policy locally to devices. if the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

10 Close the form.

11 Close the IPSec Tunnel Template form.

Procedure 29-5 To create an IPsec security policy

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the list filter parameters and click on the Search button. A list of services appears at the bottom of the Manage Services form.

3 Choose a VPRN service.

4 Click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

5 Click on the Sites tab.

6 Choose an entry and click on the Properties button. The VPRN Site (Edit) form opens with the General tab displayed.

7 Click on the IPSec Security Policies tab.

8 Click on the Create button. The IPSec Security Policy (Create) form opens with the General tab displayed.

9 Configure the parameters:

- Auto-Assign ID
- Security Policy ID

10 Click on the IPSec Security Policy Entries tab.

11 Click on the Create button. The Security Policy Entry (Create) form opens.

12 Configure the Entry ID parameter.

13 Configure the Local Address Option parameter.

14 Perform one of the following.

a If you set the Local Address Option parameter to IP Address in step 13, configure the following parameters:

- IP Address
- Prefix Length

b If you set the Local Address Option parameter to None or Any, go to step 15.

15 Configure the Remote Address Option parameter.

16 Perform one of the following.

a If you set the Remote Address Option parameter to IP Address in step 15, configure the following parameters:

- IP Address
- Prefix Length

b If you set the Remote Address Option parameter to None or Any, go to step 17.

17 Click on the OK button. The Security Policy Entry (Create) form closes.

18 Repeat steps 8 to 17 to add additional IPSec security policy entries.

19 Click on the OK button. The IPSec Security Policy (Create) form closes. A dialog box appears.

20 Click on the OK button.

21 Close the VPRN Site (Edit) form.

22 Close the VPRN Service (Edit) form.

23 Close the Manage Services form.

Procedure 29-6 To create a tunnel interface on an IES or VPRN

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the list filter parameters and click on the Search button. A list of services appears at the bottom of the Manage Services form.

3 Choose an IES or VPRN service.

4 Click on the Properties button. The IES Service (Edit) form or VPRN Service (Edit) form opens with the General tab displayed.

5 Click on the Interfaces tab. The TMS Interfaces tab is displayed.

6 Click on the Tunnel Interfaces tab.

7 Click on the Create button. The Tunnel Interface (Create) form opens with the General tab displayed.

8 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- Cflowd Type
- Configured IP MTU (Octets)

9 Configure a port for the interface.

i Click on the Port tab.

ii Click on the Select button to choose a port to associate with the tunnel interface. The Select Terminating Port - Tunnel Interface form opens.

iii Specify a filter for the search, if required, and click on the Search button.

iv Select a port from the list and click on the OK button. The Select Terminating Port - Tunnel Interface form closes and the Tunnel Interface (Create) form reappears with the port information displayed. Additional tabs appear.

v Configure the parameters:

- Auto-Assign ID
- Outer Encapsulation Value
- SAP Description
- SAP Administrative State



Note 1 — You can configure the 5620 SAM to automatically assign lowest unused outer encapsulation value by enabling the Auto-Assign ID parameter.

Note 2 — You can set the Auto-Assign ID parameter to be the default parameter for dot1 Q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter in the User Preferences form. Choose Application→ User Preferences from the main menu.

Note 3 — Private and public tunnel connection points support only dot1 Q encapsulation.

10 Configure multichassis redundancy, if required. See Procedure 37-1 in chapter 37.

11 Assign ingress and egress QoS policies to the interface, if required.

i Click on the QoS tab.

ii Configure the parameters:

- Use Shared Queue
- Use Multipoint Shared Queue

iii Click on the Select button in the Ingress Policy panel to choose an ingress QoS policy. The Select Ingress Policy - Tunnel Interface form opens.

iv Use the configurable filter and Search button to choose a policy, and click on the OK button. The Select Ingress Policy - Tunnel Interface form closes and the Tunnel Interface (Create) form reappears with the ingress QoS policy information displayed.

v Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - Tunnel Interface form opens.

vi Use the configurable filter and Search button to choose a QoS policy, and click on the OK button. The Select Egress Policy - Tunnel Interface form closes and the Tunnel Interface (Create) form reappears with the egress QoS policy information displayed.

12 Assign an accounting policy to the interface, if required.

i Click on the Accounting tab.

ii Click on the Select button to choose an accounting policy. The Select Accounting Policy - Tunnel Interface form opens.

iii Choose an accounting policy and click on the OK button. The Select Accounting Policy - Tunnel Interface form closes, and the Tunnel Interface (Create) form refreshes with the accounting policy name.

iv Configure the Collect Accounting Statistics parameter.

13 Configure scheduling, if required.

i Click on the Schedulers tab.

ii Configure the Aggregate Rate Limit (kbps) parameter.



Note 1 — The Aggregate Rate Limit (kbps) parameter is configurable only when you enable the Assign Aggregate Rate Limit check box, and there is no scheduler specified in the Egress Scheduler panel.

Note 2 — You cannot specify an egress scheduler when the Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

iii Click on the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - Tunnel Interface form opens.

iv Choose an ingress scheduler and click on the OK button. The Select Ingress Scheduler - Tunnel Interface form closes, and the Tunnel Interface (Create) form refreshes with the ingress scheduler information displayed.

v Click on the Select button in the Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - Tunnel Interface form opens.

vi Choose an egress scheduler and click on the OK button. The Select Egress Scheduler - Tunnel Interface form closes, and the Tunnel Interface (Create) form refreshes with the egress scheduler information displayed.

vii Click on the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Policer Control Policy - Tunnel Interface form opens.

viii Choose an ingress policer control policy and click on the OK button. The Select Policer Control Policy - Tunnel Interface form closes and the Tunnel Interface (Create) form refreshes with the ingress policer information displayed.

ix Click on the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Policer Control Policy - Tunnel Interface form opens.

x Choose an egress policer control policy and click on the OK button. The Select Policer Control Policy - Tunnel Interface form closes and the Tunnel Interface (Create) form refreshes with the egress policer information displayed.

14 Assign ingress and egress ACL filters to the interface, if required.

i Click on the ACL tab.

ii Click on the Select button in the Ingress Filter panel to choose an ingress IPv4 ACL filter. The Select Ingress Filter - Tunnel Interface form opens.

iii Select an ingress ACL filter and click on the OK button. The Select Ingress Filter - Tunnel Interface form closes and the Tunnel Interface (Create) form reappears with the ingress IPv4 ACL filter information displayed.

iv Click on the Select button in the Egress Filter panel to choose an egress IPv4 ACL filter. The Select Egress Filter - Tunnel Interface form opens.

v Select an egress ACL filter and click on the OK button. The Select Egress Filter - Tunnel Interface form closes and the Tunnel Interface (Create) form reappears with the egress IPv4 ACL filter information displayed.

15 Configure BFD, if required.

i Click on the BFD tab. A configuration form opens.

ii Set the Administration Status parameter to Up. The configuration form is refreshed with additional parameters.

iii Configure the parameters:

- Administration Status
- Transmit Interval
- Receive Interval
- Echo Interval
- Multiplier
- Termination Type
- Inherit from Network Element
- Operational State Transition Interval

iv To view local and remote session peers, click on the BFD Session tab. 5620 SAM retrieves information from local and remote nodes and displays a list of BFD current sessions on router interfaces or L3 interfaces.

v Click on a session. A properties form opens for the session. View the following:

- BFD status
- protocol used
- local address
- remote address
- operational status and statistics

The BFD Status field indicates one of the following:

- no service, when BFD is disabled
- in service, when BFD is running
- out of service, when BFD has failed

vi Click on the OK button.



Note — You cannot enable BFD on an interface, if BFD is not configured on the interface. You cannot set the administration status of an interface to disabled, when protocols using the interface have BFD enabled. See chapter 23 for information about enabling and disabling BFD for routing protocols.

16 Assign an IP address to the tunnel interface.

i Click on the Addresses tab.

ii Click on the Create button. The IP Address (Create) form opens.

iii Configure the parameters:

- Address ID
- IP Address
- Prefix Length

iv Click on the OK button. The IP Address (Create) form closes, and a dialog box appears.

v Click on the OK button. The Tunnel Interface (Create) form reappears with the assigned IP addresses displayed.

17 Configure an IP-IP tunnel or GRE tunnel on the Tunnel Interface, if required.

i Click on the IP/GRE Tunnels tab.

ii Click on the Create button. The IP/GRE Tunnel - IP-GRE|IP-IP Tunnel (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Name
- Description
- DSCP
- Reassembly (msec)
- Destination Address
- Remote Address
- Local Endpoint Address
- Backup Remote Address
- Configured IP MTU (Octets)
- Clear Don't Fragment Bit

iv Perform one of the following:

- If you are configuring a GRE tunnel, enable the Include GRE Header parameter.
- If you are configuring an IPv4-to-IPv4 tunnel, do not enable the Include GRE Header parameter.

v Click on the Select button on the Delivery Service panel to choose a delivery service for the tunnel. The Select Delivery Service - IP-GRE|IP-IP Tunnel form opens.

vi Select a delivery service and click on the OK button. The Select Delivery Service - IP-GRE|IP-IP Tunnel form closes and the IP/GRE Tunnel - IP-GRE|IP-IP Tunnel (Create) form reappears with the delivery service information displayed.

vii Click on the States tab and configure the Administrative State parameter.

viii Click on the OK button. The IP/GRE Tunnel - IP-GRE|IP-IP Tunnel (Create) form closes, and a dialog box appears.

ix Click on the OK button. The Tunnel Interface (Create) form reappears with the assigned GRE tunnel displayed.

18 Specify queue overrides by clicking on the Override Policy Items tab. See chapter 43 for information about how to set queue overrides.



Note — The Override Policy Items tab contains a number of sub-tabs. However, the sub-tabs that are displayed depend on the port type that you have chosen for this interface.

- If you configured a non-HSMDA port, then the Access Ingress Queues, Access Egress Queues, Ingress Policer, and Egress Policer sub-tabs are active.
- If you configured an HSMDA port, then the Access Ingress Queues, Access Egress HSMDA Queues and Ingress Policer sub-tabs are active.

19 Click on the OK button. A dialog box appears.

20 Click on the OK button. The Tunnel Interface (Create) form closes, and the IES Service (Create) or VPRN Service (Create) form reappears.

21 Repeat steps 7 to 19 to create another tunnel interface for the IES or VPRN service.

22 To create an IPSec tunnel on a VPRN tunnel interface, see Procedure 29-7.

Procedure 29-7 To create an IPsec tunnel on a VPRN tunnel interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the list filter parameters and click on the Search button. A list of services appears at the bottom of the Manage Services form.

3 Choose a VPRN service.

4 Click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

5 Click on the Interfaces tab. The TMS Interfaces tab is displayed.

6 Click on the Tunnel Interfaces tab.

7 Choose a tunnel interface and click on the Properties button. The Tunnel Interface (Edit) form opens with the General tab displayed.

8 Click on the IPsec Tunnels tab.



Note — You must first assign a port to the tunnel interface for the IPsec Tunnels tab to appear.

9 Click on the Create button. The IPSec Tunnel (Create) form opens with the General tab displayed.

10 Configure the parameters:

- Name
- Description
- Replay Window
- Keying
- Local Gateway Address
- Remote Gateway Address
- Configured IP MTU (Octets)
- Clear Don't Fragment Bit

11 Click on the Select button beside the Security Policy ID parameter. The Select Security Policy - IPSec Tunnel list form opens.

12 Specify a filter for the search, if required, and click on the Search button. A list of policies appears.

13 Choose an entry and click on the OK button. The Select Security Policy - IPSec Tunnel form closes.

14 Click on the Select button beside the Name parameter. The Select Service Name - IPSec Tunnel list form opens.

15 Specify a filter for the search, if required, and click on the Search button. A list of services appears.

16 Choose an entry and click on the OK button. The Select Service Name - IPSec Tunnel form closes.

17 Perform one of the following.

a If you set the Keying parameter to None in step 10, go to step 20.

b If you set the Keying parameter to Dynamic in step 10, go to step 18.

c If you set the Keying parameter to Manual in step 10, go to step 19.

18 Configure dynamic keying.

i Click on the Dynamic Keying tab.

ii Click on the Select button beside the following parameters:

- Transform ID 1
- Transform ID 2
- Transform ID 3
- Transform ID 4

The Select Transform ID - IPSec Tunnel form opens.

iii Specify a filter for the search, if required, and click on the Search button. A list of policies appears.

iv Choose an entry and click on the OK button. The Select Transform ID - IPSec Tunnel form closes.

v Click on the Select button beside the IKE Policy parameter. The Select IKE Policy - IPSec Tunnel list form opens.

vi Specify a filter for the search, if required, and click on the Search button. A list of policies appears.

vii Choose an entry and click on the OK button. The Select IKE Policy - IPSec Tunnel form closes.

viii Configure the parameters:

- Pre Shared Key
- Auto Establish

ix Configure the parameters in the Local ID panel:



Note — The configuration of parameters in the Local ID panel, as well as the Certificate File and Key File parameters, is only possible if IKEv2 is specified in the associated tunnel IKE policy and the Authorization Method is set to Certificate Authentication.

- Type
- Value

  The Value parameter is only displayed when the Type parameter is set to a value other than None.

x Click the Select button in the Certificate panel to select a Certificate Trust Anchor. The Select Certificate Trust Anchor list form is displayed.

xi Click on the Search button to display the list of available CA Profile names.

xii Choose the required entry and click on the OK button. The Select Certificate Trust Anchor form closes and the Name field in Certificate panel displays your selection.

xiii Configure the parameters:

- Certificate File
- Key File



Note — If there is a problem with the either the Certificate File or the Key File after the tunnel becomes administratively up, the Invalid Certificate File or Invalid Key File operational flags will indicate this in the States tab. Fault alarms will also be generated and can be checked in the Faults tab.

xiv Go to step 20.

19 Configure manual keying.

i Click on the Manual Keying tab.

ii Click on the Create button. The IPSec Security Association (Create) form opens.

iii Click on the Select button in the Security Policy Entry panel. The Select Security Policy Entry - IPSec Security Association list form opens.

iv Click on the Search button. A list of policy entries appears.

v Choose an entry and click on the OK button. The Select Security Policy Entry - IPSec Security Association list form closes.

vi Configure the parameters:

- Direction
- Encryption Key
- Authentication Key
- SPI

vii Click on the Select button in the Transform panel. The Select Transform - IPSec Security Association list form opens.

viii Click on the Search button. A list of transform policies appears.

ix Choose an entry and click on the OK button. The Select Transform - IPSec Security Association list form closes.

x Click on the OK button. The IPSec Security Association (Create) form closes.

20 Click on the States tab.

21 Configure the Administrative State parameter.

22 Click on the BFD tab.

23 Configure the parameters:

- Designated
- Enabled

If you set the Enabled parameter to Enabled, go to step 24. Otherwise, go to step 29.

24 Click on the Select button beside the Service Name parameter. The Select BFD Service - IPsec Tunnel BFD form opens.

25 Configure the filter, if required, and choose a BFD service. The BFD service information appears for the Service Name, Service ID, and Site ID parameters.

26 Click on the Select button beside the Name parameter. The Select Interface - IPsec Tunnel BFD form opens.

27 Configure the filter, if required, and choose an interface. The interface name appears for the Name parameter.

28 Configure the Destination Address parameter.

29 Click on the OK button. The IPSec Tunnel (Create) form closes. A dialog box appears.

30 Click on the OK button.

31 Repeat steps 9 to 30 to add additional IPsec tunnels.

Procedure 29-8 To create an IPsec gateway on an IES or VPRN

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the list filter parameters and click on the Search button. A list of services appears at the bottom of the Manage Services form.

3 Select an IES or VPRN.

4 Click on the Properties button. The properties form for the service opens with the general properties of the service displayed on the General tab.

5 Click on the Interfaces tab.

6 In the L3 Access Interfaces tab, click on the Search button. A list of L3 access interfaces appears.

7 Choose the L3 access interface on which you want to create the IPsec gateway and click on the Properties button. The *Service* L3 Access Interface (Edit) form opens with the General tab displayed.



Note — The port configured on the L3 access interface must be a Tunnel Group SAP. This is the public-facing interface for an IPsec tunnel.

8 Click on the IPSec Gateway tab.

9 Click on the Create button. The IPSec Gateway (Create) form opens with the General tab displayed.

10 Configure the parameters:

- Name
- Pre Shared Key

11 Click on the Select button in the IKE Policy panel to associate an IKE policy with the IPSec gateway. The Select IKE Policy - IPSec Gateway list form opens.

12 Specify a filter for the search, if required, and click on the Search button. A list of IKE policies appear.

13 Choose a policy and click on the OK button. The Select IKE Policy - IPSec Gateway list form closes.

14 Click on the Select button in the IPSec Tunnel Template panel to associate an IPsec tunnel template with the IPsec gateway. The Select IPSec Tunnel Template - IPSec Gateway list form opens.

15 Specify a filter for the search, if required, and click on the Search button. A list of IPsec tunnel templates appear.

16 Choose an IPsec tunnel template and click on the OK button. The Select IPSec Tunnel Template - IPSec Gateway list form closes.

17 Select the VPRN service site to which you are creating the IPsec tunnel from the IES or VPRN by performing the following:

i Click on the Select button in the Secure Service Id panel. The Select Secure Service Id - IPSec Gateway list form opens.

ii Specify a filter for the search, if required, and click on the Search button. A list of VPRN services appears.

iii Choose an entry and click on the OK button. The Select Secure Service Id - IPSec Gateway list form closes.

18 Select the tunnel interface on the VPRN service site to which you are creating the IPsec tunnel from the IES or VPRN by performing the following:

i Click on the Select button in the Tunnel Interface Name panel. The Select Tunnel Interface Name - IPSec Gateway list form opens.

ii Click on the Search button. A list of tunnel interfaces appears.

iii Choose an entry and click on the OK button. The Select Tunnel Interface Name - IPSec Gateway list form closes.

19 Configure the Local Gateway Address parameter.

20 Configure the parameters in the Local ID panel:



Note — The configuration of parameters in the Local ID panel, as well as the Certificate File and Key File parameters, is only possible if IKEv2 is specified in the associated gateway IKE policy and the Authorization Method is set to Certificate Authentication.

- Type
- Value

  The Value parameter is only displayed when the Type parameter is set to a value other than None.

21 Click the Select button in the Certificate panel to select a Certificate Trust Anchor. The Select Certificate Trust Anchor list form is displayed.

22 Click on the Search button to display the list of available CA Profile names.

23 Choose the required entry and click on the OK button. The Select Certificate Trust Anchor form closes and the Name field in Certificate panel displays your selection.

24 Configure the parameters:

- Certificate File
- Key File



Note — If there is a problem with the either the Certificate File or the Key File after the gateway becomes administratively up, the Invalid Certificate File or Invalid Key File operational flags will indicate this in the States tab. Fault alarms will also be generated and can be checked in the Faults tab.

25 Click on the States tab.

26 Configure the Administrative State parameter.

27 Click on the OK button. The IPSec Gateway (Create) form closes. A dialog box appears.

28 Click on the OK button to close the dialog box. The *Service* L3 Access Interface (Create) form reappears.

29 Click on the OK button to save the configuration and close the form.

30 A dialog box appears. Click on the OK button to close the dialog box.

31 Click on the OK button. A dialog box appears.

32 Click on the Yes button. The properties form for the service closes.

Procedure 29-9 To enable BFD for a static LAN-to-LAN IPsec tunnel



Note — BFD can only be enabled for the 7750 SR and 7450 ESS in mixed mode.

1 On the private side, use the CLI to specify a tunnel as the BFD tunnel and enable BFD on the tunnel. For example:

```
config>service>vprn>ipsec-if>sap>tun>

[no]bfd-enable [service-id] interface interface-name dst-ip
ip-addr

[no]bfd-designated
```

See the device documentation for more information about the CLI commands.

2 On the public side, use the CLI to configure the transmit interval. For example:

```
config>service>vprn>if>

bfd transmit-interval [receive receive-interval] [multiplier
multiplier] [echo-receive echointerval]
```

See the device documentation for more information about the CLI commands.

3 Create a VPRN service. See chapter 71 for more information.

4 Create two VPRN L3 access interfaces. See chapter 71 for more information.

5 Create a tunnel interface on a VPRN, as described in Procedure 29-6.

6 Create an IPsec tunnel on a VPRN tunnel interface, as described in Procedure 29-7.

29.9 IPsec VPN procedures

The following procedures describe how to perform 5620 SAM IPsec configuration tasks using the IPsec VPN step forms.

Procedure 29-10 To create an IPsec VPN



Note — The 5620 SAM does not support the creation of IPsec VPNs when language localization is active. See "Localized language support" for more information about language localization.

1 Configure a corporate service. Table 29-2 lists where to find information about each corporate service type.

Table 29-2 Corporate service types

Corporate service	See chapter
Apipe	67
Cpipe	
Fpipe	
Ipipe	
VPLS	68
IES	70
VPRN	71
VLAN	66

2 If required, configure one or more service templates. Table 29-2 lists where to find more information.

3 Choose Manage→Service→IPsec VPNs from the 5620 SAM main menu. The Manage IPsec VPNs form opens.

4 Click on the Create button. The IPSec VPN (Create) form opens.

5 Configure the parameters:

- Auto-Assign ID
- IPsec VPN Name
- Description
- Service Type
- Link Corporate and Secured Service

6 To select a corporate service, perform the following, otherwise, go to step 7.

i Click on the Select button beside the Corporate Service ID parameter. The Select Corporate Service - IPsec VPN form opens. Only the specific service type, as set by the Service Type parameter, is listed.

ii Filter the corporate services, if required, and select a corporate service.

iii Click on the OK button to close the Select Corporate Service - IPSec VPN form. The Corporate Service ID and Corporate Service Name parameters display the service ID and service name for the selected corporate service on the Create IPsec VPN step form.

7 Click on the Next button on the Create IPsec VPN step form. The Select Service Sites step form opens. Perform Procedure 29-11 to select the service sites.

Procedure 29-11 To select a service NE site for an IPsec VPN

This procedure selects the NE site for the IPsec VPN.

1 Perform Procedure 29-10 to create an IPsec VPN.

2 Perform one of the following:

a To choose an existing service site, configure the filter and click on the Search button. A list of service sites appears. Go to step 7.

b To create a service site, go to step 3.

3 Click on the Create button. The Manage Equipment form opens.

4 Configure the filter, if required, and click on the Search button. A list of NEs appears.

5 Select a NE and click on the OK button. The NE appears in the Select Service Sites step form.

6 Repeat steps 3 to 5 to add another NE site.

7 Select an NE site and click on the Next button. The Create/Select Secure VPRN Service step form opens. Perform Procedure 29-12 to:

- select a service
- create a service
- create a service from a template

Procedure 29-12 To create or select a secure VPRN service for an IPsec VPN

1 Perform Procedures 29-10 and 29-11.

2 Perform one of the following:

a To select a service, go to step 3.

b To create a service, go to step 7.

c To create a service from a template, go to step 12.



Note — The template must be configured for one site. The template cannot be used if the template is configured for multiple sites.

3 Click on the Select Service button. The Select Service form opens.

4 Configure the filter, if required, and click on the Search button. A list of services appear.

5 Select a service and click on the OK button. The service appears in the Create/Select Secure VPRN Service step form.

6 Click on the Service Site tab and configure the parameters:

- Description
- Administrative State

Go to step 15.

7 Click on the Create Service button.

8 Click on the Select button beside the Customer parameter. The Select Customer form opens.

9 Filter the customers, if required, and select a customer from the list.

10 Click on the OK button.

11 Configure the parameters:

- Service Name
- Description
- Service Tier
- Administrative State

Go to step 6.

12 Click on the Create Service From Template button. The Create Service From Template appears.

13 Filter the services, if required, and click on the Search button.

14 Select a service from the list and click on the OK button. Go to step 6.

15 Click on the Next button. The Create/Select Delivery Service(s) step form opens. Perform Procedure 29-13.

Procedure 29-13 To create or select a delivery service for an IPsec VPN

1 Perform Procedures 29-10 to 29-12.

2 Perform one of the following:

- **a** To select a delivery service, go to step 3.
- **b** To create a delivery service, go to step 8.
- **c** To create a service from a template, go to step 13.



Note — The template must be configured for one site. The template cannot be used if the template is configured for multiple sites.

- **d** To remove a service, go to step 17.

3 Click on the Select Service button. The Select Service form opens.

4 Choose IES Service (IES) or VPRN Service (VPRN) from the drop-down menu, choose a filter, if required, and click on the Search button.

5 Select a service from the list and click on the OK button. The service appears in the Create/Select Delivery Service(s) list.

6 Click on the Service Site tab and configure the parameters:

- Description
- Administrative State

7 Repeat steps 3 to 6 to select another service. Go to:

- **a** step 8 to create a service
- **b** step 13 to create a service from a template
- **c** step 17 to remove a service
- **d** step 18 to select a tunnel group

8 Click on the Create Service button and choose VPRN or IES. The service appears in the Create/Select Delivery Service(s) list.

9 Click on the Select button beside the Customer parameter. The Select Customer form opens.

10 Choose a customer and click on the OK button.

11 Configure the parameters:

- Service Name
- Description
- Service Tier
- Administrative State

12 Repeat steps 8 to 11 to create another service. Go to:

a step 13 to create a service from a template

b step 17 to remove a service

c step 18 to select a tunnel group

13 Click on the Create Service From Template button and choose VPRN or IES. The Create Service From Template form appears.

14 Configure the filter, if required, and click on the Search button. A list of services appears.

15 Select a service template and click on the OK button.

16 Repeat steps 13 to 15 to create another service. Go to:

a step 17 to remove a service

b step 18 to select a tunnel group

17 If you perform this step, the service is removed without confirmation and there is no undo. Select a service in the Create/Select Delivery Service(s) list and click on the Remove Service button.

18 Click on the Next button. The Tunnel Group Selection step form opens. Perform Procedure 29-14.



Note — The Next button is not enabled until you perform steps 9 and 10 for each delivery service in the Create/Select Delivery Service(s) step form.

Procedure 29-14 To select a tunnel group for an IPsec VPN

1 Perform Procedures 29-10 to 29-13.

2 Select a service and configure the parameters by clicking in the panel and entering values or choosing an option:



Note 1 — The parameters are not part of the XML. In OSSI, you can create the ServiceSiteStructs and in the ServiceSiteStructs, you can create the IPsec VPN objects.

Note 2 — If the tunnel type is static, the parameters that require configuration are:

- Delivery Service Interface Address
- Local Gateway Address
- Remote Gateway Address
- Static Route Address
- Static Route Prefix

If the tunnel type is dynamic site-site, the parameters that require configuration are:

- Delivery Service Interface Address
- Local Gateway Address

If the tunnel type is dynamic soft client, the parameters that require configuration are:

- Secure Service Interface Address
- Delivery Service Interface Address
- Local Gateway Address

- ISA-Tunnel Group
- Tunnel Type
- Secure Service Interface Address
- Delivery Service Interface Address
- Local Gateway Address
- Remote Gateway Address
- Static Route Address
- Static Route Prefix

3 Click on the Service Site tab and configure the parameters:

- Description
- Administrative State

4 Repeat steps 2 and 3 for each service.

5 Click on the Next button. The Create Policy step form opens.

Perform Procedure 29-15 if you chose Dynamic (Site-to-Site) for the Tunnel Type parameter in step 2.

Perform Procedure 29-16 if you chose Dynamic (Soft Client) for the Tunnel Type parameter in step 2.

Perform Procedure 29-17 if you chose Static for the Tunnel Type parameter in step 2.



Note — The Next button is not enabled until you perform step 2 for each tunnel group in the Tunnel Group Selection step form.

Procedure 29-15 To assign policies and configurations for a dynamic site-to-site IPsec VPN

This procedure assumes you chose Dynamic (Site-to-Site) for the Tunnel Type parameter in step 2 of Procedure 29-14.

1 Perform Procedures 29-10 to 29-14.

2 Click on the Select button beside the IPsec Tunnel Template Policy ID parameter in the IPsec Tunnel Template panel. The Select IPsec Tunnel Template - IPsec VPN form opens.

3 Perform one of the following:

- **a** To select an IPsec tunnel template from the list, go to step 4.
- **b** To create an IPsec tunnel template, go to step 5.

4 Configure the filter, if required, click on the Search button. Go to step 10.

5 Click on the Create button. The IPsec Tunnel Template form opens. Perform steps 3 to 11 in Procedure 29-4.

6 Click on the Select button beside the Policy ID parameter in the IKE Policy panel. The Select IKE Policy - IPsec VPN form opens.

7 Perform one of the following:

- **a** To select an IKE Policy from the list, go to step 9.
- **b** To create an IKE Policy, go to step 8.

8 Click on the Create button and perform steps 3 to 12 in Procedure 29-1.

9 Select a Policy and click on the OK button.

10 Configure the Pre Shared Key parameter.

11 Click on the Finish button.

If there is a configuration problem, the Problems Encountered form opens. Fix the problem and click on the Finish button.

If there are no configuration problems, a completed message appears. The 5620 SAM performs the following:

- a secure VPRN service and sites are created (see Code 29-1)
  - an access interface is created
  - a tunnel interface is created
  - the service name is configured
- the IES or VPRN delivery service and sites are created (see Code 29-2)
  - an access interface is created
  - the IP address of the SAP is configured
  - a tunnel group with an auto-generated outer encapsulation as a public SAP is assigned
  - an IPsec gateway is created
  - the secure service is assigned
  - the tunnel interface of the secure service is assigned
  - the tunnel template is assigned
  - the IKE policy is assigned
  - the local gateway address is configured
  - the Pre Shared key is configured
  - the service name is configured
- if the Link Corporate and Secure Service parameter is enabled, a composite service is created that contains the corporate and secure service

You can click on the View the newly created IPSec Secured VPN button. The IPsec VPN form opens.

Code 29-1: Secure VPRN service example

```
vprn 254 customer 2 create
            ipsec-interface "sam-auto-ipsec-intf-1" create
                sap ipsec-2.private:9 create
                exit
            exit
            service-name "VPRN service-310 CPM_132_A (38.120.169.132)"
            no shutdown
        exit
```

Code 29-2: VPRN delivery service example

```
vprn 255 customer 2 create
            interface "sam-auto-access-intf-1" create
                address 33.33.3.3/24
                sap ipsec-2.public:11 create
                    ipsec-gw "sam-auto-gateway-1"
                        default-secure-service 254 ipsec-interface
"sam-auto-ipsec-intf-1"
                        default-tunnel-template 1
                        ike-policy 1
                        local-gateway-address 33.33.3.2
                        pre-shared-key "Test"
                        no shutdown
                    exit
                exit
            exit
```

```
    service-name "VPRN service-311 CPM_132_A (38.120.169.132)"
    no shutdown
exit
```

Procedure 29-16 To assign policies and configurations for a dynamic soft client IPsec VPN

This procedure assumes that you chose Dynamic (Soft Client) for the Tunnel Type parameter in step 2 of Procedure 29-14.

1. Perform Procedures 29-10 to 29-14.
2. Perform steps 2 to 9 in Procedure 29-15.
3. Click on the Select button beside the Displayed Name parameter. The Select Subscriber Authentication Policy - IPsec VPN form opens.
4. Perform one of the following:
   - **a** To select a subscriber authentication policy from the list, go to step 6.
   - **b** To create a subscriber authentication policy, go to step 5.
5. Click on the Create button. The Subscriber Authentication Policy (Create) form opens. See the *5620 SAM System Administrator Guide* for information about creating a Subscriber Authentication Policy.
6. Select a subscriber authentication policy from the list and click on the OK button.
7. Click on the Finish button.

   If there is a configuration problem, the Problems Encountered form opens. Fix the problem and click on the Finish button.

If there are no configuration problems, a completed message appears. The 5620 SAM performs the following:

- a secure VPRN service and sites are created (see Code 29-3)
  - an access interface is created
  - a tunnel interface is created
  - the IP Address of the SAP is configured
  - the service name is configured
- the IES or VPRN delivery service and sites are created (see Code 29-4)
  - an access interface is created
  - the IP address of the SAP is configured
  - the RADIUS authentication policy is assigned
  - a tunnel group with an auto-generated outer encapsulation as a public SAP is assigned
  - an IPsec gateway is created
  - the tunnel template is assigned
  - the IKE policy is assigned
  - the local gateway address is configured
  - the Pre Shared key is configured
  - the service name is configured
- if the Link Corporate and Secure Service parameter is enabled, a composite service is created that contains the corporate and secure service

You can click on the View the newly created IPSec Secured VPN button. The IPsec VPN form opens.

Code 29-3: Secure VPRN service example

```
vprn 260 customer 2 create
            ipsec-interface "sam-auto-ipsec-intf-4" create
                address 9.9.9.9/24
                sap ipsec-1.private:47 create
                exit
            exit
            service-name "VPRN service-316 CPM_132_A (38.120.169.132)"
            no shutdown
        exit
```

Code 29-4: VPRN delivery service example

```
vprn 261 customer 2 create
            interface "sam-auto-access-intf-4" create
                address 40.1.1.2/24
                authentication-policy "test"
                sap ipsec-1.public:42 create
                    ipsec-gw "sam-auto-gateway-4"
                        default-tunnel-template 1
                        ike-policy 2
                        local-gateway-address 40.1.1.1
                        pre-shared-key "Test"
                        no shutdown
                    exit
                exit
            exit
```

```
    service-name "VPRN service-317 CPM_132_A (38.120.169.132)"
    no shutdown
exit
```

Procedure 29-17 To assign policies and configurations for a static IPsec VPN

This procedure assumes that you chose Static for the Tunnel Type parameter in step 2 of Procedure 29-14.

1 Perform Procedures 29-10 to 29-14.

2 Perform steps 3 to 6 in Procedure 29-15.

3 Configure the parameters:

- Pre Shared Key
- Replay Window
- Keying

If you set the Keying parameter to Manual, go to step 4. If you set the Keying parameter to Dynamic, go to step 6.

4 Configure the Manual Keying - Inbound parameters:

- Keying Type
- Encryption Key
- Authentication Key
- SPI Inbound

5 Configure the Manual Keying - Outbound parameters:

- Keying Type
- Encryption Key
- Authentication Key
- SPI Outbound

6 Perform one of the following:

a To select an IPsec transform policy from the list, go to step 8.

b To create an IPsec transform policy, go to step 7.

7 Click on the Create button and perform steps 3 to 12 in Procedure 29-1.

8 Select an IPsec transform policy and click on the OK button.

9 Configure the Auto Establish parameter.



Note — The Auto-Establish parameter is only configurable if dynamic keying is selected.

10 Click on the Finish button.

If there is a configuration problem, the Problems Encountered form opens. Fix the problem and click on the Finish button.

If there are no configuration problems, a completed message appears. The 5620 SAM performs the following:

- a secure VPRN service and NE sites are created (see Code 29-5)
  - the IPsec security policy is created
  - a tunnel interface is created
  - a tunnel group with an auto-generated outer encapsulation as a private SAP is assigned
  - the IPsec tunnel is created
  - the security policy is assigned to the tunnel
  - the local and remote gateway addresses are configured
  - the delivery service is configured
  - the replay window is configured
  - the keying is configured
  - if set, auto establish is enabled
  - the static route is configured
  - the service name is configured
- the IES or VPRN delivery service and NE sites are created (see Code 29-6)
  - an access interface is created
  - a tunnel group with an auto -generated outer encapsulation as a public SAP is assigned
  - the IP address of the SAP is configured
  - the service name is configured
- if the Link Corporate and Secure Service parameter is enabled, a composite service is created that contains the corporate and secure service

You can click on the View the newly created IPSec Secured VPN button. The IPsec VPN form opens.

Code 29-5: Secure VPRN service example - Keying parameter set to Dynamic

```
vprn 252 customer 2 create
            ipsec
                security-policy 1 create
                    entry 1 create
                        local-ip any
                        remote-ip any
                    exit
                exit
            exit
            ipsec-interface "sam-auto-ipsec-intf-32" create
```

```
                sap ipsec-1.private:46 create
                    tunnel "sam-auto-tunnel-32" create
                        security-policy 1
                        local-gateway-address 40.1.1.2 peer 2.2.2.2 delivery-service
253
                        replay-window 64
                        dynamic-keying
                            ike-policy 1
                            pre-shared-key "Test"
                            transform 1
                        exit
                        no shutdown
                    exit
                exit
            exit
            static-route 3.3.3.3/32 ipsec-tunnel "sam-auto-tunnel-32"
            service-name "VPRN service-308 CPM_132_A (38.120.169.132)"
            no shutdown
        exit
```

Code 29-6: VPRN delivery service example

```
vprn 253 customer 2 create
            interface "sam-auto-access-intf-32" create
                address 40.1.1.1/24
                sap ipsec-1.public:41 create
                    collect-stats
                exit
            exit
            service-name "VPRN service-309 CPM_132_A (38.120.169.132)"
            no shutdown
        exit
```

30 — ISA-Video

30.1 ISA-Video overview *30-2*

30.2 Workflow to configure and manage an ISA-Video configuration *30-3*

30.3 ISA-Video procedures *30-4*

30.1 ISA-Video overview

The 5620 SAM supports, on a 7450 ESS or 7750 SR, the equipment and service configuration of the following enhancements to multicast video services based on the ISA-Video MDA:

- Reliable Delivery/Retransmisson (RT) Proxy
- Fast Channel Change (FCC)
- Ad Insertion (ADI)

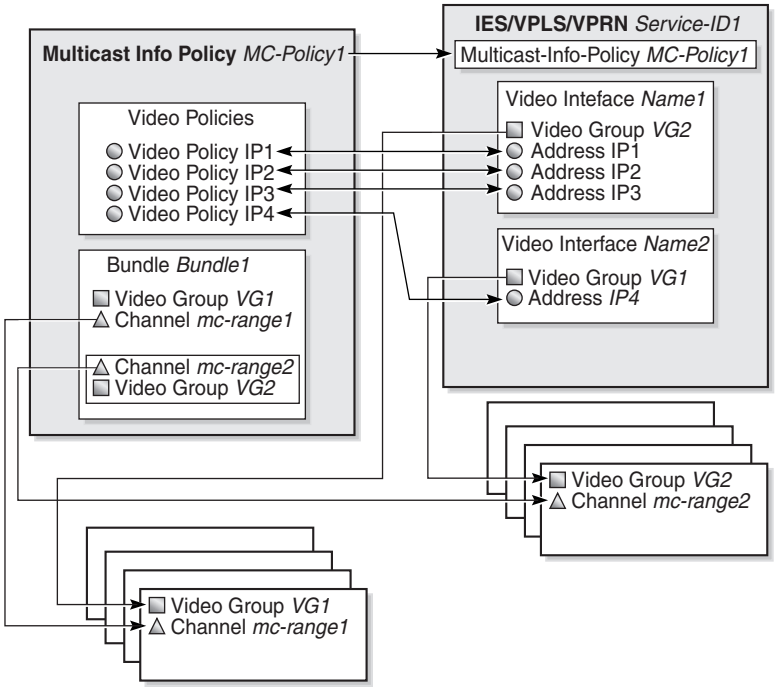
You can use the 5620 SAM to configure the required ISA-Video Groups and Members, as well as the associated multicast info policies. VPRN, IES, and VPLS services can then be configured for the customer video delivery.

These enhancements are provisioned in 5620 SAM in following three areas:

- A Video Group configuration to manage the ISA resources and service grouping.
- Multicast Information policy configuration parameters and objects to handle the RT, FCC and Ad insertion capabilities, including:
  - A Video Policy configuration under the Multicast Information Policy
  - Video parameters added to Multicast Bundles, Channels and Channel override configurations
- Video Interface configurations are added under VPRN/IES/VPLS services sites.

Figure 30-1 shows the relationship of these various elements and how they are associated through configuration.

Figure 30-1 ISA-Video configuration elements



A Video Interface within a service site can have up to eight IP addresses. The IP addresses assigned to a Video Interface determine which MultiCast Info Policy is applied. The Video Group you assign to the Video Interface determines which bundle/channel configuration inside the Multicast Info policy is applied to the interface. You also configure the ingress and egress QOS policies for the Video Interface using the Video Group.

If a request is received on a Video Interface for a channel not serviced by the Video Group associated with that specific Video Interface, then the request is considered invalid and is dropped. For example, in Figure 30-1, a request for mc-range2 received on IP1, IP2, or IP3 is invalid. A request for mc-range2 is only valid on IP4.

A Video Group manages the ISA-Video MDA resource and the configurations of the enhanced video functionality. You can assign a Video Group (for example, VG1 in Figure 30-1) for each Bundle, and this is the default Video Group for all of the channels in that Bundle. You can then apply specific configuration overrides for each channel within a Video Group assignment.

Up to four Video Groups (ID 1-4) can be configured on a single NE. Each Video Group in turn, can have multiple primary video ISAs assigned to provide load balancing and redundancy protection. However, any specific video ISA can only be bound to one Video Group. The binding of a video ISA to the Video Group is referred as a Video Group Member.

Additional considerations for the Ad Insertion functionality:

- Ingress Ad Insertion channels are configured on the Video Interface configuration form.
- If Ad Insertion functionality is enabled on a Video Group, then the group can only have one Video Group Member.
- You can configure Zone Channels for egress Ad Insertion on each Ad Insertion channel configuration.
- Ad Insertion channels are not applicable to VPLS.

30.2 Workflow to configure and manage an ISA-Video configuration

1. Provision the ISA-Video MDA. See chapters 12 and 13 for more information about ISA-Video MDA equipment configuration.
2. Create or configure ISA-Video Groups and add members under the Video Groups. See Procedure 14-7 for more information.
3. Configure and distribute a global Multicast Information policy. Configure the channel bundle, channel range, channel overrides, and video interface for the NE. See Procedure 45-4 for more information.
4. Create and enable a video interface for the VPLS, IES, or VPRN service. See Procedures 30-1, 30-2, and 30-3 for more information.

30.3 ISA-Video procedures

The following procedures describe how to perform 5620 SAM ISA-Video configuration tasks.

Procedure 30-1 To add a Video interface to a VPRN site

The 7710 SR and 7750 SR support the configuration of a video interface in a VPRN service.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose the required VPRN service and click on the Properties button. The VPRN (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site to which you want to add the video interface; expand the entries for that site.

5 Right-click on the Video Interfaces and choose Create Video Interface. The Video Interface (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Name
- Description
- Administrative State
- Group Number
- Associated Multicast Service ID
- RT Client Address
- ADI Administrative Status
- SCTE 30 Control Address
- SCTE 30 Data Address

After you choose a Group Number, the following selectable fields are also displayed:

- Ingress QoS Policy
- Egress QoS Policy
- Ingress IP Filter
- Egress IP Filter

Choose the required policies and filters by clicking on the Select button beside the corresponding fields. You can perform a search or choose the entry from the list that appears for each of these items.

7 Click on the Security tab.

8 Click on the Select button and choose the required NE DoS Protection Policy from the list. You can also perform a search from this form.

9 Click on the Addresses tab and click on the Create button. The IP Address (Create) form opens.

10 Configure the parameters:

- IP Address
- Address Type
- Prefix Length

11 Go to step 12 if you are configuring ad insertion. Otherwise go to step 25.

12 Click on the ADI Channels tab and click on the Create button. The Video ADI Channel (Create) form opens with the General tab displayed.

13 Configure the parameters:

- Name
- Description
- Multicast Channel IP Address
- Unicast Source IP Address
- SCTE 35 Action

14 Click on the Zone Channels tab and click on the Create button. The Video ADI ZoneChannel (Create) form opens.

15 Configure the parameters:

- Name
- ADI Zone Multicast Address
- ADI Zone Unicast Source Address

16 Click on the OK button. The Video ADI ZoneChannel (Create) form closes, and a dialog box appears.

17 Click on the OK button. The Video ADI Channel (Create) form reappears, with the newly-configured Zone Channels displayed in the list.

18 Repeat steps 14 to 17 to configure additional Zone Channels, if required.

19 Click on the OK button. The Video ADI Channel (Create) form closes, and a dialog box appears.

20 Click on the OK button. The Video Interface (Create) form reappears with the newly-configured ADI Channels displayed in the list.

21 Click on the ADI (SCTE 30) Server tab and click on the Create button. The ADI (SCTE 30) Server (Create) form opens.

22 Configure the Server Address parameter.

23 Click on the OK button. The ADI (SCTE 30) Server (Create) form closes and a dialog box appears.

24 Click on the OK button. The ADI (SCTE 30) Server form reappears with the newly-configured ADI (SCTE 30) Server displayed in the list.

25 Click on the OK button. The Video Interface (Create) form closes and a dialog box appears.

26 Click on the OK button. The newly-configured Video Interface is displayed for the site.

27 Close the Manage Services form.

Procedure 30-2 To add a Video interface to an IES site

The 7710 SR and 7750 SR support the configuration of a video interface in an IES.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose the required IES service and click on the Properties button. The IES Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site to which you want to add the video interface and expand the entries for that site.

5 Right-click on the Video Interfaces and choose Create Video Interface. The Video Interface (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Name
- Description
- Administrative State
- Group Number
- Associated Multicast Service ID
- RT Client Address
- ADI Administrative Status
- SCTE 30 Control Address
- SCTE 30 Data Address

After you select a Group Number, the following selectable fields are also displayed:

- Ingress QoS Policy
- Egress QoS Policy
- Ingress IP Filter
- Egress IP Filter

Choose the required policies and filters by clicking on the Select button adjacent to the corresponding fields. You can conduct a search or choose the required entry from the list that appears for each of these items.

7 Click on the Security tab.

8 Click on the Select button to select the required NE DoS Protection Policy from the list displayed in the form. You can also conduct a search from this form.

9 Click on the Addresses tab and click on the Create button. The IP Address (Create) form opens.

10 Configure the parameters:

- IP Address
- Address Type
- Prefix Length

11 Go to step 12 if you are configuring ad insertion. Otherwise go to step 25.

12 Click on the ADI Channels tab and click on the Create button. The Video ADI Channel (Create) form opens with the General tab displayed.

13 Configure the parameters:

- Name
- Description
- Multicast Channel IP Address
- Unicast Source IP Address
- SCTE 35 Action

14 Click on the Zone Channels tab and click on the Create button. The Video ADI ZoneChannel (Create) form opens.

15 Configure the parameters:

- Name
- ADI Zone Multicast Address
- ADI Zone Unicast Source Address

16 Click on the OK button. The Video ADI ZoneChannel (Create) form closes and a dialog box appears.

17 Click on the OK button. The Video ADI Channel (Create) form reappears, with the newly-configured Zone Channels displayed in the list.

18 Repeat steps 14 to 17 to configure additional Zone Channels, if required.

19 Click on the OK button. The Video ADI Channel (Create) form closes and a dialog box appears.

20 Click on the OK button. The Video Interface (Create) form reappears with the newly-configured ADI Channels displayed in the list.

21 Click on the ADI (SCTE 30) Server tab and click on the Create button. The ADI (SCTE 30) Server (Create) form opens.

22 Configure the Server Address parameter.

23 Click on the OK button. The ADI (SCTE 30) Server (Create) form closes and a dialog box appears.

24 Click on the OK button. The ADI (SCTE 30) Server form reappears with the newly-configured ADI (SCTE 30) Server displayed in the list.

25 Click on the OK button. The Video Interface (Create) form closes and a dialog box appears.

26 Click on the OK button. The newly-configured Video Interface is displayed for the site.

27 Close the Manage Services form.

Procedure 30-3 To add a Video interface to a VPLS site

The 7710 SR and 7750 SR support the configuration of a video interface in a VPLS.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose the required VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site to which you want to add the video interface and expand the entries for that site.

5 Right-click on the Video Interfaces and select Create Video Interface. The Video Interface (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Name
- Description
- Administrative State
- Group Number
- Associated Multicast Service ID
- RT Client Address
- Gateway Address

After you select a Group Number, the following selectable fields are also displayed:

- Ingress QoS Policy
- Egress QoS Policy
- Ingress IP Filter
- Egress IP Filter
- Ingress Mac Filter
- Egress Mac Filter

Choose the required policies and filters by clicking on the Select button adjacent to the corresponding fields. You can conduct a search or choose the required entry from the list that appears for each of these items.

7 Click on the Security tab.

8 Click on the Select button to select the required NE DoS Protection Policy from the list displayed in the form. You can also conduct a search from this form.

9 Click on the Addresses tab and click on the Create button. The IP Address (Create) form opens.

10 Configure the parameters:

- IP Address
- Address Type
- Prefix Length

11 Click on the OK button. The Video Interface (Create) form closes, and a dialog box appears.

12 Click on the OK button. The newly-configured Video Interface is displayed for the site.

13 Close the Manage Services form.

31 — Alarm management

31.1 Alarm management overview *31-2*

31.2 Workflow to manage alarms *31-15*

31.3 Alarm management procedures *31-17*

31.1 Alarm management overview

The 5620 SAM converts SNMP traps from NEs and 5620 SAM events to alarms that are associated with the managed equipment, configured services and policies. The alarm-based fault management system provides the following:

- conversion of SNMP traps from NEs to alarms using the X.733 standard
- correlation of alarms with equipment- and service-affecting faults
- updates to the managed-object operational status in near-real-time
- alarm policy control that allows a network administrator to specify how to process alarms, and how to create and store the alarm logs
- point-and-click alarm management using the 5620 SAM GUI dynamic alarm list and object properties forms
- the ability to log the actions performed to resolve a related fault by adding notes to the alarm
- alarm history for performing trend analysis

Figure 31-1 shows how the 5620 SAM manages alarms.

Figure 31-1 Alarm management

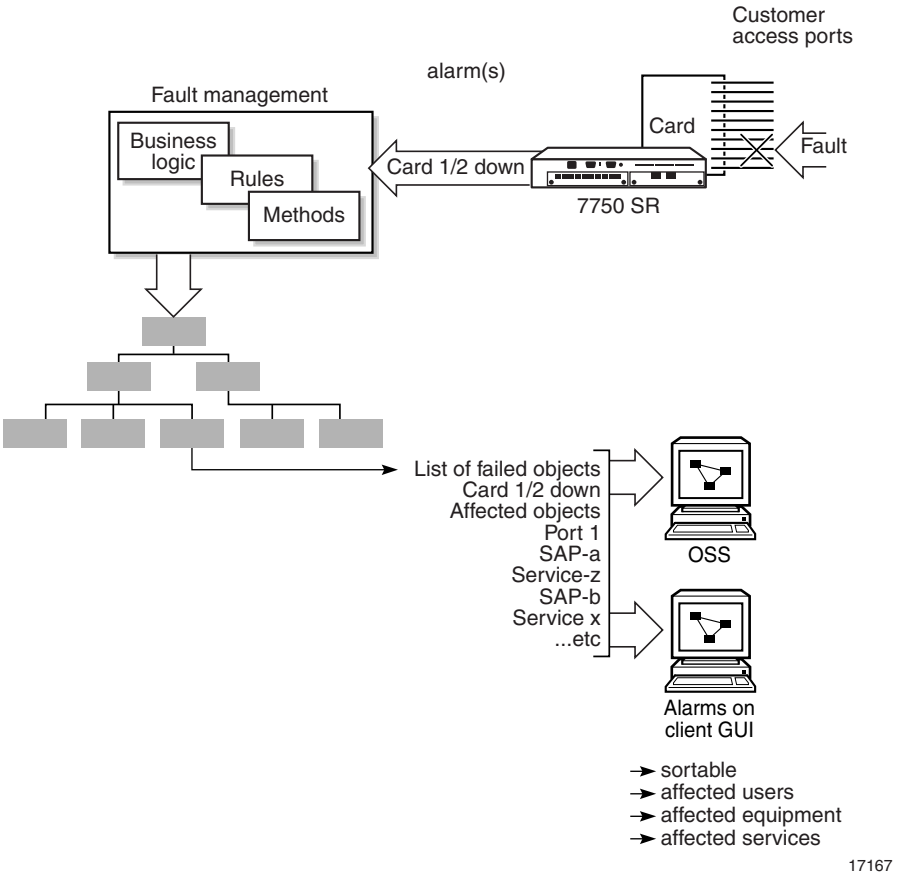
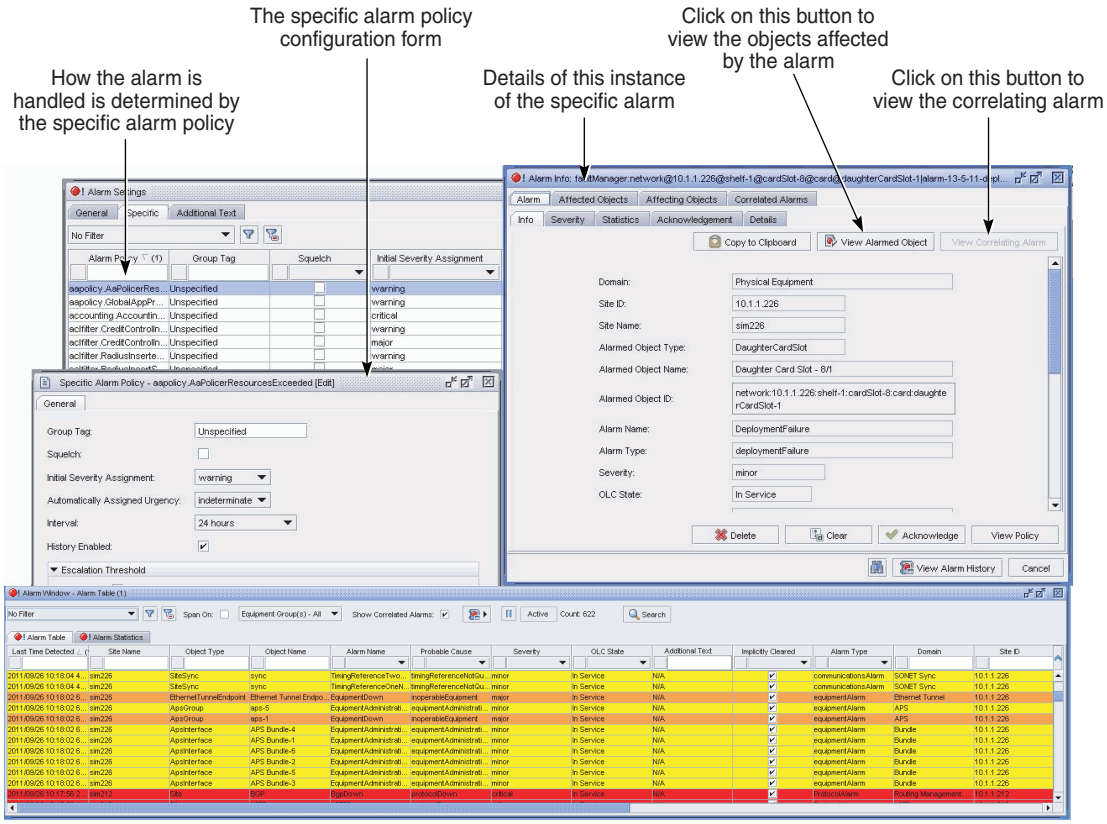


Figure 31-2 shows the following alarm objects in the 5620 SAM GUI:

- an incoming alarm in the dynamic alarm list
- the alarm policy
- the alarm information form

Figure 31-2 Alarm relationships on the GUI



You can view alarm information and manage alarms from the following areas of the 5620 SAM GUI:

- The Alarm Window, which displays the incoming network alarms in the dynamic alarm list.
- The Faults tab on object properties forms, which lists alarms for a selected object.
- The Alarm Info form, which contains detailed information about a specific alarm.

The following tabs appear on an Alarm Info form, as shown in Figure 31-2.

- Alarm tab—contains alarm information under Info, Severity, Statistics, Acknowledgement, and Details subtabs
- Affected Objects tab—lists objects that are affected by the alarm even when correlation alarm suppression is enabled. Figure 31-3 shows how affected objects are determined.

- Affecting Objects tab— lists objects that directly affect the object of the alarm. Figure 31-3 shows how affecting objects are determined.
- Correlated Alarms tab—lists correlated alarms, which are generated for other objects that depend on the alarmed object

You can view the history of one or more alarms using a 5620 SAM menu option, the Alarm Info form, or the contextual menu in the Alarm Window or Faults tab list. From the alarm window, you can choose the More Actions→Historical Alarms option to open the Historical Alarms form. You can view the alarm history of an object by choosing the View Object(s) Alarm History contextual menu option.



Note — The View Alarm(s) History and View Object(s) Alarm History menu options are not available when more than 20 alarms are selected.

Table 31-1 describes the types of alarm information available.

Table 31-1 Alarm Information

Field name or column heading	Description
Acknowledged	Whether the alarm has been acknowledged by an operator. A check mark indicates acknowledgement.
Acknowledged By	Name of the operator who acknowledged the alarm
Additional Text	The Additional Text information includes information for the following objects based on configured policies: • Itself—The type of object from which the attribute was selected. • Its Children—Object types that are contained by the source; for example, children for a service include the site and access interface. • Its Association—Dynamic relationships between object types that are not related hierarchically. For example, access interfaces and ports, LAGs and ports, and composite services and their components along with various types of services. Associations are calculated based on the context of the managed network. Associations change as the network topology changes. Use the summary tool to display the current associations for an object type. • Its Peers—A peer is an object type that is contained by the same generic abstract class as the source. For example, peers of a VPLS are VPRN, IES, VLL-EPIPE, VLL-CPIPE, and mirror services. These peers are contained by the generic 'service' abstract class. See Procedure 31-5.
Alarm Name	Name of the alarm
Alarm Policy	Name of the alarm policy
Alarm Type	Vendor-specific and X.733 standards for the event type of the alarm
Alarmed Object ID	A unique string that identifies the object down to the lowest level; for example, network ID #, chassis #, slot #, and daughterCardSlot #
Alarmed Object Name	The name of the alarmed object as it appears in the navigation tree
Alarmed Object Type	The type of object against which the alarm is raised
Cleared By	The username of the operator who last cleared the alarm
Clearing Condition	The condition that clears the alarm

(1 of 3)

Field name or column heading	Description
Correlating Alarm ID	A unique string that identifies the correlating alarm
Current Severity	The current severity level of the alarm
Custom Text	The custom text added to the specific policy for the alarm. Click on the ... button if required to display the entire custom text entry. You can add up to 256 characters of custom text to an alarm policy. See Procedure 31-3 for more information.
Description	A description of the alarm. If the information is more than 250 characters, click on the ... button to display the entire description.
Domain	The general area of the 5620 SAM software that is affected by the alarm. Domain is of specific interest and use to those monitoring alarms using the XML OSS interface.
First Time Detected(1)	The clock time of the first recorded instance of the alarm
Frequency	The number of occurrences of the alarm during the last interval. The interval is specified in the alarm policy. You can modify the alarm frequency by clicking on the View Policy button and configuring the specific alarm policy. See Procedure 31-3 for more information.
Highest Severity	The highest severity assigned to the alarm. Alarm severity can change based on the escalation policies.
Implicitly Cleared	Indicates whether the alarm is cleared by the 5620 SAM or by an operator. Self-clearing alarms are automatically cleared from the alarm list after the condition that triggered the alarm no longer exists. The Implicitly Cleared field identifies self-clearing alarms with a check mark.
Last Time Acknowledged	The clock time when the alarm was most recently acknowledged
Last Time Cleared(1)	The clock time when the alarm was most recently cleared
Last Time De-escalated(1)	The clock time for the last time that the alarm was de-escalated. Alarm escalation/de-escalation occurs when alarm severity is automatically changed based on the frequency of the alarm in a specified interval, as defined by an alarm policy. See Procedures 31-1 and 31-3.
Last Time Demoted(1)	The clock time for the last time that the alarm was demoted to a lower severity. Alarm promotion/demotion refers to manual changes to alarm severity. See Procedures 31-1 and 31-3.
Last Time Detected(1)	The clock time of the most recent recorded instance of the alarm. This field provides useful information when multiple instances of the same alarm are raised.
Last Time Escalated(1)	The clock time for the most recent time that the alarm was escalated. Alarm escalation/de-escalation occurs when alarm severity is automatically changed based on the frequency of the alarm in a specified interval, as defined by an alarm policy. See Procedures 31-1 and 31-3.
Last Time Promoted(1)	The clock time for the most recent time that the alarm was promoted to a higher severity. Alarm promotion/demotion refers to manual changes to alarm severity. See Procedures 31-1 and 31-3.
Last Time Severity Changed(1)	The clock time for the most recent time that the alarm severity was changed
Number of Correlated alarms	The number of correlated alarms. See "Correlated alarms" in this section.
Number of Occurrences	The number of occurrences of the alarm. As each new instance of the alarm is raised, the number of occurrences statistic increases, and the Last Time Detected field displays the time that the last instance of the alarm was raised.

(2 of 3)

Field name or column heading	Description
Number of Occurrences Since Acknowledged	The number of occurrences of the alarm since it was most recently acknowledged
Number of Occurrences Since Clear	The number of occurrences of the alarm since it was most recently cleared
Object ID	A unique string that identifies the object down to the lowest level; for example, network ID #, chassis #, slot #, and daughterCardSlot #
Object Name	The name of the alarmed object as it appears in the navigation tree
Object Type	The type of object against which the alarm is raised
OLC State	The configured Object Life Cycle state.
Original Severity	The severity level of the alarm when it was first raised
Previous Severity	The previous severity level of the alarm
Previously Acknowledged	A check mark indicates that the alarm was previously acknowledged
Probable Cause	The vendor-specific and X.733 probable cause of the alarm
Raising Condition	The condition that caused the alarm to be raised
Remedial Action	The action required to clear the alarm. If the information is more than 250 characters, click on the ... button to display the complete text.
Service Affecting	Indicates whether the fault affects network traffic to end users. This field only applies to the 1830 PSS.
Severity	The vendor-specific, TMN, and X.733 standards for severity of the alarm. See "Alarm status, severity, and aggregation" in this section.
Site ID	One of the following: • IP address of the NE that raises the alarm • IP address of the 5620 SAM main or auxiliary server that raises the alarm; in a redundant deployment, the active main or auxiliary server
Site Name	One of the following: • name of the NE that raises the alarm • hostname of the 5620 SAM main or auxiliary server that raises the alarm; in a redundant deployment, the active main or auxiliary server
Urgency	The operator-assigned level of importance for managing the alarm. The options are: • indeterminate • minor • major • critical
Urgency Assigned By	The username of the operator who assigned the urgency level.

(3 of 3)

Note

(1) When the field includes (NE Time), the NE clock time is displayed, which may differ from the Client Time. (NE Time) applies to 9471 WMM and eNodeB alarms.

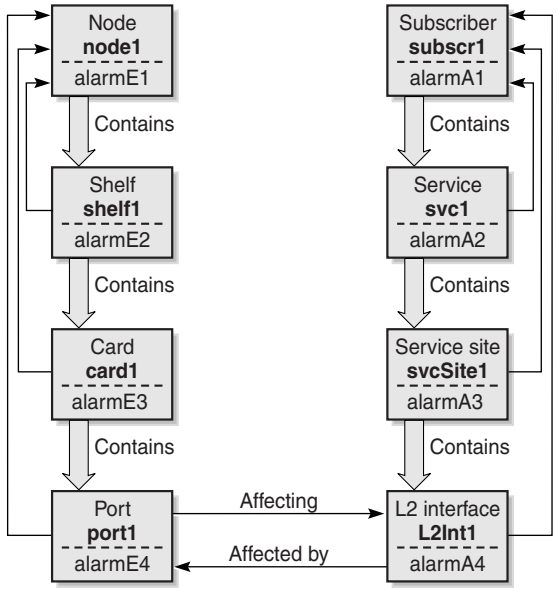
Alarm status, severity, and aggregation

The alarm status for the network appears in the navigation tree, dynamic alarm list, and topology maps. You can use the navigation tree to view the status of an alarm generated for a specific object and to view the aggregated alarm status. When one or more alarms are generated for a specific object or related object, an indicator appears on the Faults tab on the object properties form. The indicator does not provide the severity of the alarm, it only specifies that an alarm exists.

Alarms are related or affecting when there is a relationship between objects. The 5620 SAM determines that, for example, if a port goes down and the port is used by a SAP, a customer is affected by the port down alarm.

Figure 31-3 shows how aggregation, affecting, and affected alarms are determined.

Figure 31-3 Aggregation, affecting, and affected alarm inheritance



- **L2Int1** depends on the **port1**.
- **port1** affects **L2Int1**
- alarmE4 affects **L2Int1**

18023

Table 31-2 lists the alarm relationships based on the example in Figure 31-3.

Table 31-2 Alarm relationships

Object	Object alarms	Affecting alarms	Aggregated alarms	Related object alarms
NE1	alarmE1	—	alarmE2 alarmE3 alarmE4	—
shelf1	alarmE2	—	alarmE3 alarmE4	—
card1	alarmE3	—	alarmE4	—
port1	alarmE4	—	—	alarmA4
subscr1	alarmA1	—	alarmA2 alarmA3 alarmA4	—

(1 of 2)

Object	Object alarms	Affecting alarms	Aggregated alarms	Related object alarms
svc1	alarmA2	—	alarmA3 alarmA4	—
svcSite1	alarmA3	—	alarmA4	—
L2Int1	alarmA4	alarmE4	—	—

(2 of 2)

The 5620 SAM GUI uses color to indicate alarm severity. The color code is used consistently throughout the GUI; for example, in the navigation tree, dynamic alarm list, and topology maps. Table 31-3 lists the default alarm colors.

Table 31-3 Default 5620 SAM alarm colors

Alarm severity	Default color
Critical	Red
Major	Orange
Minor	Yellow
Warning	Cyan
Condition	Mocha
Cleared/Normal	Green
Indeterminate	White
Information	Light blue

The following tabs are on the Faults tab of an object properties form. When a tab contains one or more alarms, an indicator appears on the tab and on the containing Faults tab. The indicator does not represent the severity of the alarm.

- Object Alarms—contains information about the alarm as viewed from the dynamic alarm list. For example, shelf1 is the object, and alarmE2 is the object alarm.
- Affecting Alarms—contains information about the alarms on objects that directly affect this object. For example, alarmE4 on object port1 affects object L2Int1, because of the relationship between the L2 interface and the port.
- Aggregated Alarms—contains alarm information for objects below the listed object in the containment hierarchy. For example, object shelf1 contains two propagated alarms, alarmE3 and alarmE4, because the shelf contains card1 and port1.
- Alarms on Related Objects—contains information about the alarms that have an indirect relationship with the object. For example, alarmA4 is displayed in this tab for port1, because the alarm is related to the fault condition on port1.

Figure 31-4 shows the alarm status information for an object in the navigation tree, the object properties form, and the associated alarm information form. You can use the alarm information form to view the affected objects, the affecting objects, and the correlated alarms.

Note — An aggregated alarm may appear in the navigation tree even when no child object in the tree has an alarm. This is because the navigation tree is a filter for different views. When you change the view using the drop-down menu, for example, from Equipment to Network, the aggregated alarm on the child object may appear.

Figure 31-4 Alarm status information in the navigation tree

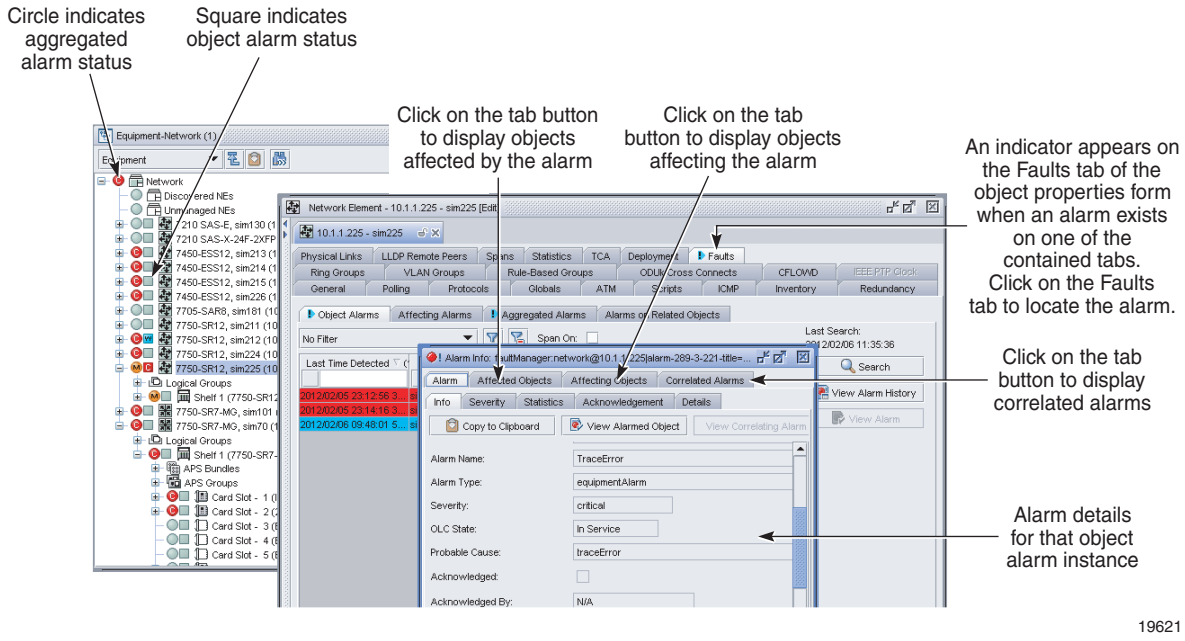


Figure 31-5 shows alarm and status information on a topology map icon. See "Troubleshooting alarms using topology maps" in the *5620 SAM Troubleshooting Guide* for more information.

Figure 31-5 Alarm and status information on topology map icons

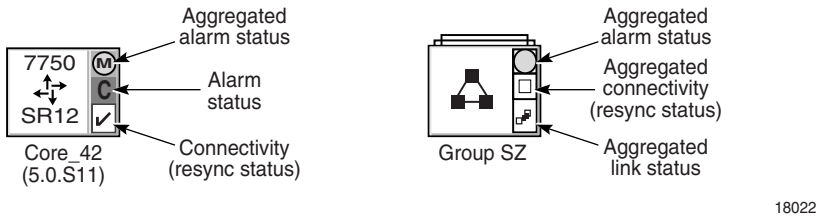
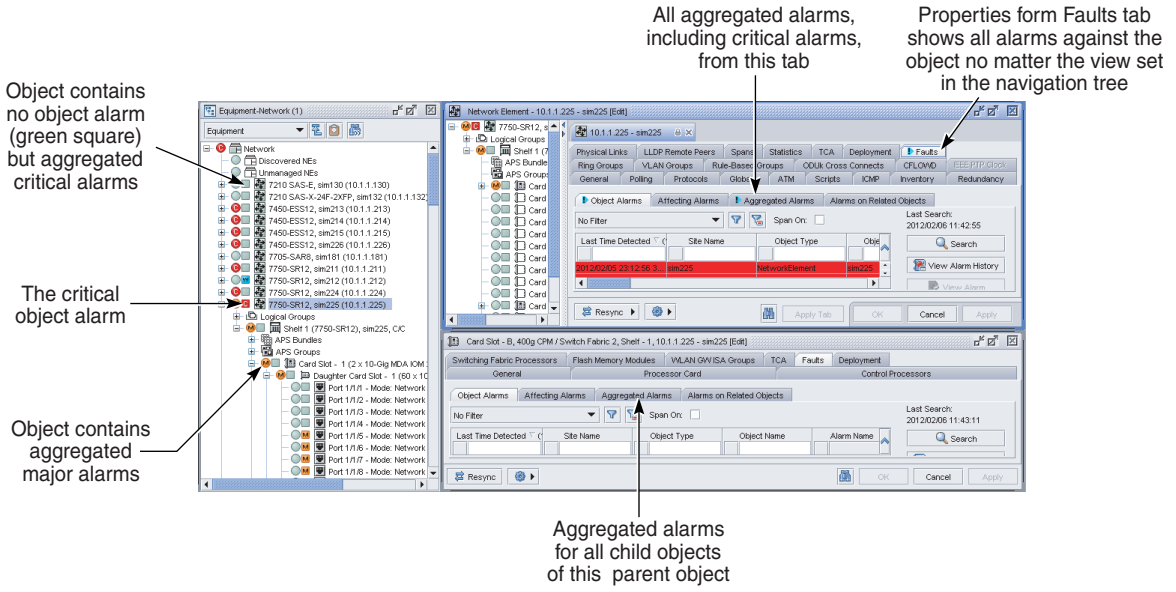


Figure 31-6 shows how to navigate from the aggregated or object alarms in the navigation tree to the Faults tab of an object properties form.

Figure 31-6 Navigating from the navigation tree to Faults tab on a properties form

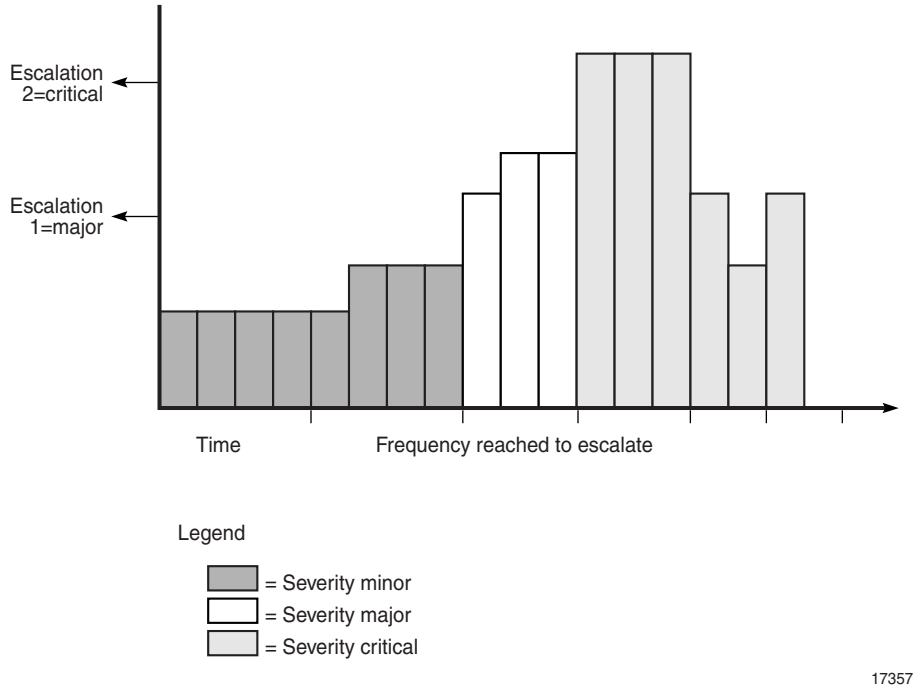


Alarm thresholds

The 5620 SAM provides configurable alarm parameters to escalate and de-escalate the severity of alarms, as described in Procedure 31-3.

Figure 31-7 shows an example of what happens when an alarm threshold escalation is reached, and a policy is applied. Figure 31-8 shows two escalation and two de-escalation policies applied to an alarm.

Figure 31-7 Alarm thresholds without de-escalation policies

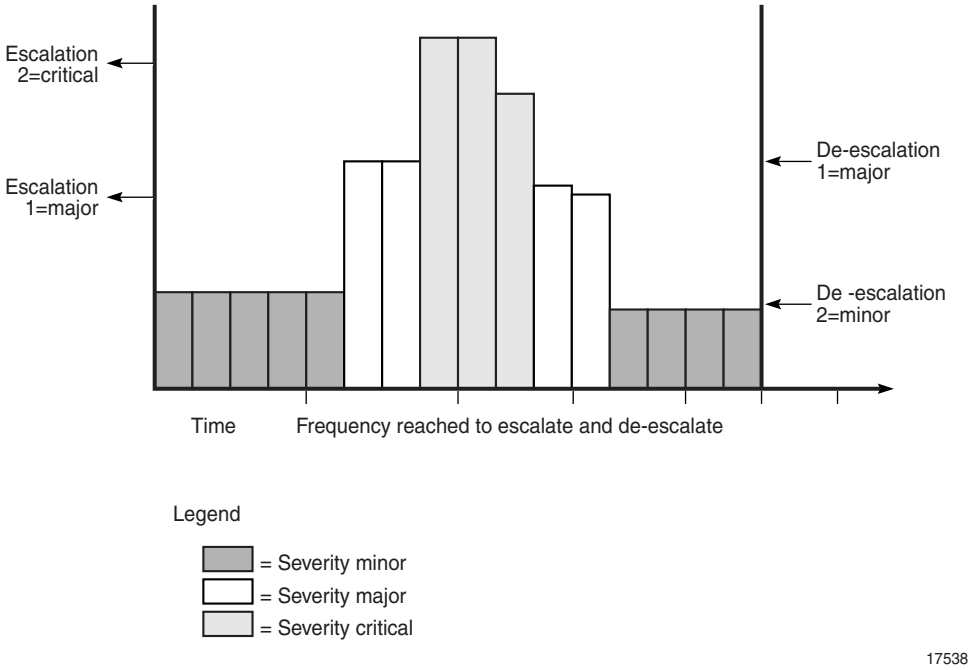


The preceding figure shows two escalation policies applied to an alarm. Escalation rules are applied when the number of instances of the alarm, also called the frequency, reaches the configured value. De-escalation rules are applied when the number of instances of the alarm is less than the configured frequency value. If the escalation value is reached, the alarm is escalated to the configured value. As shown in the figure, the first escalation is to major priority and then to critical priority. When the appropriate frequency to escalate and de-escalate is reached, the alarm is first escalated in severity and then de-escalated. However, if the alarm is deleted, then the frequency calculation is affected.

Note — When no de-escalation policy is applied, escalated alarms are not de-escalated once the frequency of the alarm is less than the alarm escalation threshold.

Figure 31-8 shows two escalation and two de-escalation policies applied to an alarm.

Figure 31-8 Alarm thresholds with de-escalation policies



Escalation policies are affected by the Auto Deletion Rule parameter of the global alarm deletion policy. See Procedure 31-1 for more information. When an escalation policy uses the “Delete Alarms when Cleared” default option for the Automatic Alarm Deletion Settings parameter, the escalation policy is not applied. You must configure the parameter to a value other than “Delete Alarms when Cleared” to ensure that the escalation policy is applied.

Alarm suppression

The 5620 SAM is designed to not generate alarms when numerous SNMP traps are sent in quick succession for the same type of event. This prevents alarm storms during intermittent outages in the network caused by bouncing NEs; for example, if links go up and down rapidly. The 5620 SAM continues to resynchronize the network. If the bouncing NEs continue to send down state SNMP traps, the 5620 SAM eventually receives the trap and generates the appropriate alarm.

To indicate how often an alarm is generated, the number of occurrences of each instance of the alarm is tracked in the alarm record of the initial alarm. Click on the Statistics tab of an Alarm Info form to display how often the alarm was generated.

To escalate the alarm severity if an alarm reoccurs a specific number of times, use the threshold crossing alert functionality. Configure the escalation or the de-escalation parameter as described in Procedure 31-3.

The 5620 SAM uses a trap throttling process to prevent the 5620 SAM system from being overloaded with traps if a failure occurs. Trap throttling does not affect the sequencing of traps. The trap throttling process allows the 5620 SAM to process traps when time permits. As a result, the 5620 SAM keeps track of the traps that the software missed and resynchronizes only the missed traps. Trap throttling is supported and configured using the CLI on each Alcatel-Lucent NE. See the Alcatel-Lucent NE System Management Guides for configuration information.

Alarm filters

You can create and specify filters to view network alarms in the dynamic alarm list. You can save multiple filters and view the alarm information by opening up to six alarm windows. The name of the filter appears in the alarm window title of each alarm window that is open. See Procedure 31-16.

Filtering alarms for OSS clients using the 5620 SAM GUI

You can configure a filter to allow OSS clients to search for alarms using the 5620 GUI. See Procedure 31-7 and the *5620 SAM XML OSS Interface Developer Guide*.

Consider the following when you use the 5620 SAM GUI to assign alarm filters to OSS clients:

- Only public filters can be applied to OSS clients.
- When a user logs in to the 5620 SAM GUI, filters that were created for OSS applications are not applied to GUI alarms.
- Filters that are applied using the 5620 SAM GUI apply only to the fault (5620-SAM-topic-xml-fault) and filter (5620-SAM-topic-xml-filtered) JMS topics.
- When the 5620 SAM GUI is used to apply or remove a filter, you do not need to disconnect or reconnect an OSS session.
- When a filter is defined and enabled, and the client does not have an OSS connection, the filter is applied when the OSS client connects.
- When a filter is defined and enabled, and the user has one or more OSS connections, the filter is applied to all of the user OSS connections.
- When an alarm filter is in use with an OSS session and a 5620 SAM user changes the contents of the filter, the 5620 SAM user is informed that the filter is in use and who is using the filter. The 5620 SAM user is prompted with the option to save the change or cancel the change.
- Alarm filters that are applied to OSS sessions appear in the Sessions tab on the 5620 SAM User Security-Security Management form.

Correlated alarms

The 5620 SAM generates a correlated alarm when a fault condition on one object causes an alarm condition on another object. For example, if a port goes down, an alarm is generated for the port, which is the affected object. Each service that uses the port generates an alarm. The alarm information for the affected object includes the correlated alarms.

The 5620 SAM automatically promotes the severity of correlating alarms to match the severity of correlated alarms. For example, if a major correlating port alarm has one or more critical correlated service alarms, the 5620 SAM changes the severity of the correlated port alarm to critical. The correlating alarm cannot have a severity that is lower than the severity of the correlated alarms. However, the severity that is defined by a specific alarm policy takes precedence over the correlated severity. The 5620 SAM does not lower the severity of correlating alarms when correlated alarms are cleared.



Note — Alarm correlation does not affect the severity of HIP alarms, or alarms that originate from an external EM system.

When the event that initiates an affected object alarm is resolved and the alarm clears, the correlated alarms also clear. If a correlated alarm does not clear after the affected object alarm clears, the source of the correlated alarm is an event other than the initiating event. In this case, the alarm correlation is removed and the alarm is displayed in the dynamic alarm list. See Procedure 31-15 for information about viewing correlated alarms.

You can enable or disable the display of correlated alarms to reduce the number of alarms that appear in the dynamic alarm list. Correlated alarms are displayed by default and can be enabled or disabled for each 5620 SAM client. See Procedure 31-11 for more information.



Note — The display of correlated alarms in the alarm window does not affect the alarm status displayed in the navigation tree and topology map.

Automatic deletion of correlated alarms

You can configure the 5620 SAM to automatically delete correlated alarms when the correlating alarm is deleted, as described in Procedure 31-1. You can also configure 5620 SAM alarm settings to specify whether a user notification is displayed before you delete one or more correlated alarms.

To prevent cleared alarms from persisting in the 5620 SAM, alarm severity is not promoted by alarm correlation when you choose one of the following options for automatic alarm deletion. The options disable the correlation of alarm severity in the 5620 SAM network.

- Disable Automatic Alarm Deletion
- Delete Alarms when Acknowledged
- Delete Alarms when Cleared and Acknowledged



Note — A correlated alarm is not deleted after the deletion of the correlating alarm if there is another correlating alarm associated with the correlated alarm. Therefore, the number of correlated alarms that are automatically deleted may be less than the number in the warning notification to a GUI operator.

Service and transport alarm correlation

The 5620 SAM provides limited service and transport alarm correlation. When an LSP goes out of service, the 5620 SAM generates an alarm for the LSP and a correlated alarm for each LSP path that is a child object of the LSP. The LSP alarm is listed as an aggregated alarm for each SDP that uses the LSP. A 5620 SAM operator can use the aggregated LSP alarm for SDP troubleshooting.

There may not be a direct relationship between an LSP and the SDPs that use the LSP. For example, when LDP over RSVP is the transport mechanism, the 5620 SAM does not correlate SDP alarms with LSP alarms.

Automatic purging of alarms

Because a large number of outstanding alarms can affect system performance, the 5620 SAM purges outstanding alarms. The alarm purge algorithm sorts alarms using the following criteria:

- correlated alarms are deleted before root alarms
- lower severity alarms are deleted before higher severity alarms
- oldest alarms are deleted first

When an alarm policy does not exist, the 5620 SAM purges alarms as follows:

- If the outstanding alarm count reaches 45 000, the 5620 SAM:
  - raises an alarm to indicate that an alarm purge is in progress
  - purges non-critical and non-root alarms to the historical alarm log until the count drops to 45 000
  - displays “Max alarm count exceeded” in the status bar
- If the outstanding alarm count reaches 60 000, the 5620 SAM:
  - raises an alarm to indicate that an alarm purge is in progress
  - purges alarms to the historical alarm log, starting with the lowest severity alarms and then progressing to the oldest alarms, until the count drops to 45 000

To ensure that purged alarms are logged, you must enable alarm history logging. See Procedure 31-2 for information about configuring alarm history logging and purging policies.

31.2 Workflow to manage alarms

1. Configure the managed NEs to send SNMP fault and event traps to the 5620 SAM, as required. See the appropriate NE documentation.
2. Configure the 5620 SAM system-wide alarm settings, as required to meet your specific operational requirements. These changes affect all users. You must have a user account with the administrator scope of command role to perform these procedures.
   a. Enable or disable alarm severity and alarm deletion settings and customize their default values; see Procedure 31-1.
   b. Configure when alarms are logged to the alarm history database; see Procedure 31-2.

c Customize the default behavior of specific alarm policies; see Procedure 31-3.

d Enable or disable the display of the Additional Text Button on object properties forms; see 31-4.

e Configure additional text policies; see Procedure 31-5.

f Configure a policy to clear an alarm that is not implicitly cleared; see Procedure 31-6.

g Configure alarm filters for OSS clients using the 5620 SAM GUI; see Procedure 31-7.

h Reload alarms to ensure that the alarm service cache is up-to-date and synchronized with the historical alarm database; see Procedure 31-8.

3 Configure 5620 SAM GUI alarm user preferences, as required.

a Enable or disable audible alarms; see Procedure 31-9.

b Enable or disable the display of alarm flags in the alarm window; see Procedure 31-10.

c Enable or disable the display of correlated alarms in the alarm window; see Procedure 31-11.

d Enable or disable the display of alarmed equipment in navigation trees for the View Alarmed Object function; see Procedure 31-12

4 View and manage alarms to monitor incoming faults from network objects and the 5620 SAM.

a View and manage network alarms in the Alarm window; see Procedure 31-13.

b View and manage object alarms on object properties forms; see Procedure 31-14.

c View and manage alarms using the Alarm Info form; see Procedure 31-15.

5 Create and apply search filters to locate and view specific network alarms in the Alarm window; see Procedure 31-16.

6 Acknowledge alarms, enter notes, and change the severity of alarms, as required:

a Acknowledge alarms using the contextual menu on alarm lists; see Procedure 31-17.

b Acknowledge alarms using the Alarm Info form; see Procedure 31-18.

c Change the severity of alarms; see Procedure 31-19.

7 Perform additional alarm management functions, as required.

a List the current and historical alarms for a specific time period; see Procedure 31-20.

b Search for alarms received during a specified time period; see Procedure 31-21.

c Pause the dynamic alarm list from scrolling when viewing alarms; see Procedure 31-22.

d Copy alarm information to the clipboard for use in other applications; see Procedure 31-23.

8 View network alarm statistics. See Procedure 31-24.

9 Review historical alarm records in the alarm history log for trend analysis and view the source of alarms, and to store alarm records, as required.

a Review historical alarm records; see Procedure 31-25.

b View the source object of an historical alarm; see Procedure 31-26.

c Save lists of logged historical alarm records; see Procedure 31-27.

10 For information about troubleshooting using alarms, see "Troubleshooting using network alarms" in the *5620 SAM Troubleshooting Guide*.

31.3 Alarm management procedures

Use the following procedures to perform alarm management tasks.

Procedure 31-1 To configure alarm severity and deletion behavior

Perform this procedure to enable or disable alarm severity settings and alarm deletion settings and to specify the behavior for severity changes and alarm deletions.

You must have a user account with the administrator scope of command role or write access to the fm.GlobalPolicy class to perform this procedure.

1 Choose Administration→Alarm Settings from the 5620 SAM main menu. The Alarm Settings form opens with the General tab displayed.

2 In the Alarm Severity Settings panel, enable or disable alarm severity settings and specify the behavior for automatic and manual alarm settings.

   i Configure the Enable Severity Settings parameter, as require. You cannot configure additional parameters in the Alarm Severity Settings panel unless the parameter is enabled.

   ii Configure the parameters in the Manual pane, as required:

   - Enable Manual Severity Settings
   - Allow Manual Severity Promotions
   - Allow Manual Severity Demotions
   - Allow Manual Clearing of Automatically Clearing (Self Clearing) Alarms

   iii Configure the parameters in the Automatic pane, as required:

   - Enable Automatic Severity Settings
   - Allow Automatic Severity Promotions
   - Allow Automatic Severity Demotions
   - Allow Policy Based Escalation
   - Allow Policy Based De-escalation

3 In the Alarm Deletion Settings panel, enable or disable alarm deletion settings and specify the behavior for manual and automatic alarm deletion settings.

   i Configure the Enable Deletion Settings parameter, as required. You cannot configure parameters in the Alarm Deletion Settings panel unless the parameter is enabled.

   ii Choose one of the following options for Manual Alarm Deletion Settings:

   - Delete Alarms when Acknowledged
   - Delete Alarms when Cleared and Acknowledged
   - Delete Alarms without Restriction
   - Delete Alarms when Cleared
   - Delete Alarms when Cleared or Acknowledged
   - Disable Manual Alarm Deletion

iii Choose one of the following options for Correlated Alarm Settings for Manually Deleted Alarms:

- Delete its Correlated Alarms with GUI Notification
- Delete its Correlated Alarms without GUI Notification
- Do Not Delete any of its Correlated Alarms

iv Choose one of the following options for Automatic Alarm Deletion Settings:

- Delete Alarms when Acknowledged
- Delete Alarms when Cleared and Acknowledged
- Disable Automatic Alarm Deletion
- Delete Alarms when Cleared
- Delete Alarms when Cleared or Acknowledged



Caution — Deleting an alarm resets the frequency of the alarm to 1. This may cause conflicts with configured alarm escalation and de-escalation policies.

4 See Procedure 31-2 for information about configuring parameters in the Alarm History DB Behavior panel.

5 To reset all parameters on the General tab to their default values, click on the Reset to Default button, if required.

6 Click on the Apply button to save the changes. A dialog box appears.

7 Click on the Yes button.

8 Click on the Cancel button to close the form.

Procedure 31-2 To configure alarm history database management behavior

The 5620 SAM stores alarms in the alarm history database for record-keeping and trend analysis. You can specify when alarms are logged to the alarm history database.



Note — When the maximum number of alarms allowed in the alarm history database is reached, the oldest alarms are deleted. If you need to save information about the alarms, save a file that contains the alarm log information, as described in Procedure 31-27.

1 Choose Administration→Alarm Settings from the 5620 SAM main menu. The Alarm Settings form opens with the General tab displayed.

2 Configure the following parameters from the Alarm History DB Behavior panel:

- Administrative State
- Log On Change
- Log On Deletion



Note — Alcatel-Lucent recommends that you enable the Log on Deletion parameter to ensure that the alarm history log records all deleted alarms.

3 To reset all parameters on the General tab to their default values, click on the Reset to Default button, if required.

4 Click on the Apply button to save the changes. A dialog box appears.

5 Click on the Yes button.

6 Click on the Cancel button to close the form.

Procedure 31-3 To customize the default behavior of specific alarm policies

Perform this procedure to customize the default behavior of specific alarm policies to meet your specific operational requirements.

1 Choose Administration→Alarm Settings from the 5620 SAM main menu. The Alarm Settings form opens.

2 Click on the Policies tab. A list of alarm policies appears.

3 Choose an alarm type or multiple alarms. The alarm types are listed by *domain.alarm name*.

4 Click on the Properties button. The Specific Alarm Policy (Edit) form opens.

5 Configure the general alarm type parameters.

- Group Tag
- Squelch
- Initial Severity Assignment
- Automatically Assigned Urgency
- Interval
- History Enabled
- Auto Deletion Rule
- Custom Text

6 Configure the alarm type escalation parameters, as required. You can escalate or de-escalate the severity of an alarm based on how frequently the alarm is processed by the 5620 SAM.

i Select the Escalation or the De-escalation parameter.

ii Click on the Add button.

iii Configure the Frequency parameter. The frequency is the threshold in a 24-h period of how often the alarm must arrive before the severity is escalated or de-escalated. The alarms are analyzed at faster, non-configurable intervals to determine whether the Frequency value is reached.

iv Configure the Severity parameter to specify a different severity to be applied to the alarm if the escalation or de-escalation threshold is reached.

v Click on the OK button. The new escalation or de-escalation policy is applied to the alarm.

7 Click on the OK button to save the changes and close the Specific Alarm Policy (Edit) form. A dialog box appears.

8 Click on the Yes button.

Procedure 31-4 To display the Additional Text Find button on object properties forms

You can optionally display the Additional Text Find button (icon) on object properties forms to view alarms associated with the object.

1 Choose Administration→Alarm Settings from the 5620 SAM main menu. The Alarm Settings form opens with the General tab displayed.

2 Click on the Additional Text tab.

3 Enable or disable the Show Additional Text icon on Properties Forms parameter. See Figure 31-9.

4 Click on the OK button and close the Alarm Settings form. A dialog box appears.

5 Click on the Yes button.

Procedure 31-5 To configure additional text policies

You can configure an additional text policy to display specific information about an alarmed object in the additional text column of the dynamic alarm list and on the Alarm Info form. The Additional Text information includes information for the following objects based on configured policies:

- Itself—The type of object that the attribute was selected.
- Its Children—Object types that are contained by the source. For example, children for a service include site and access interface.
- Its Association—Dynamic relationships between object types that are not related hierarchically. For example, access interfaces and ports, LAGs and ports, composite services and their components along with various types of services. Associations are calculated based on the context of the managed network. Association changes as the network topology changes. Use the summary tool to see the current associations for an object type.
- Its Peers—A peer is an object type that is contained by the same generic abstract class as the source. For example, peers of a VPLS service are VPRN, IES, VLL-EPIPE, VLL-CPIPE, mirror services. All these peers are contained by the generic 'service' abstract class.

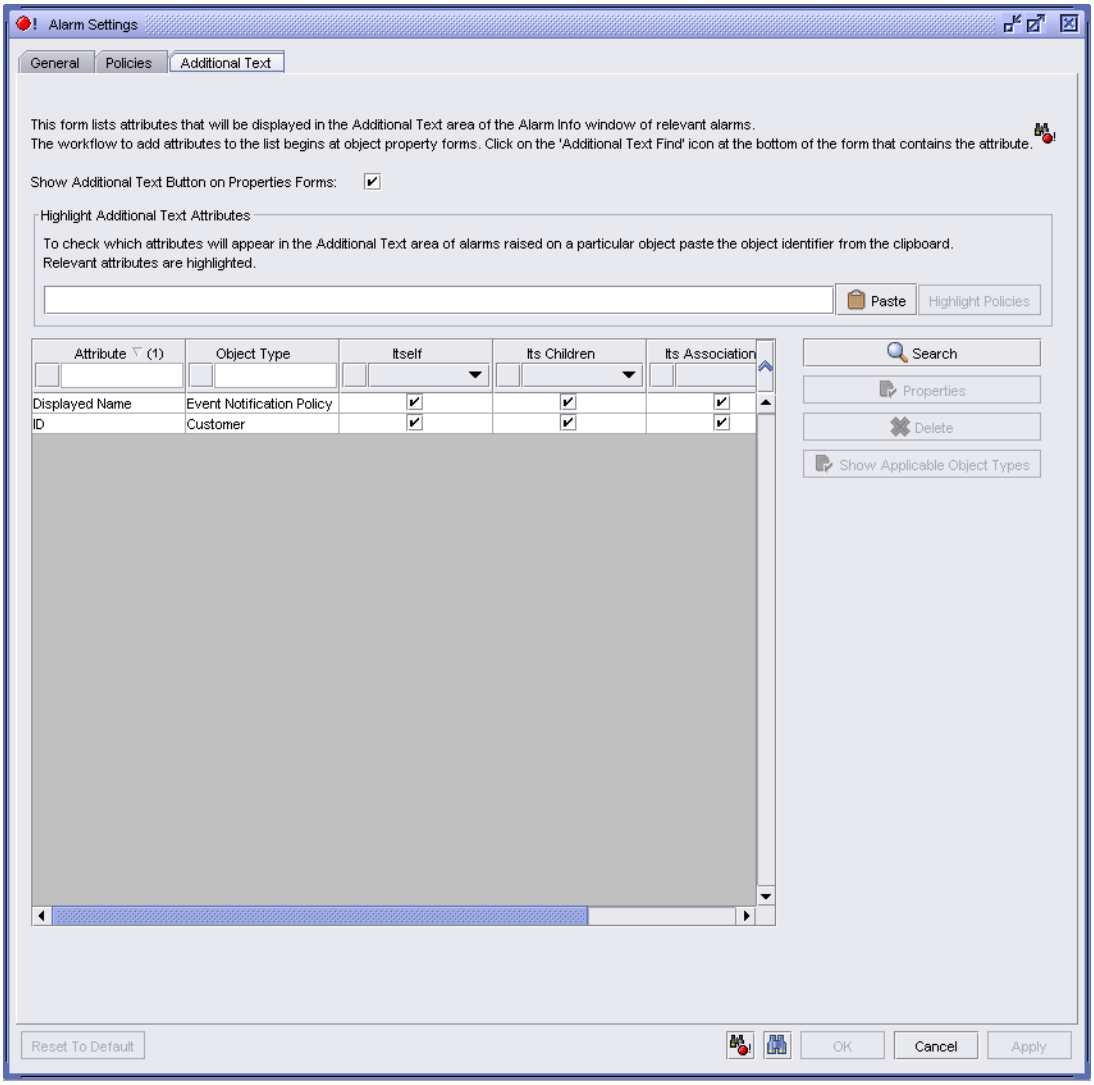


Note — You must select Its Associations for mirrored attributes to appear on an object's alarm form.

Examples of mirrored attributes on service and NE property forms:

- Example 1: On a Services Property form, choose General→Customer→ID and select the Additional Text Find icon to create an Additional text policy for a mirrored attribute for an Associating object. Enable Its Association in the Additional Text Attribute (Create) form. When an alarm is generated on the service object, the alarm will contain the Customer ID in its Additional Text field. If required, you can select Itself, and Its Children.
- Example 2: On a Network Element (Edit) property form, choose Polling→ Assigned Event Notification Policy→Name and select the Additional Text Find icon to create an Additional text policy for a mirrored attribute for an Associating object. Enable Its Association in the Additional Text Attribute (Create) form. When an alarm is generated on the NE polling object, the alarm will contain the Assigned Event Notification Policy Name in its Additional Text field. If required, you can select Itself, and Its Children.

Figure 31-9 Additional text



You may require additional information about parent objects that need to be included in alarms raised by children, for example:

- the network element name to be included in all alarms raised on the shelf, card or ports
- the service description included in all alarms raised on the site or SAP or SDP of a service

- alarms generated on each service component including the composite service name and ID
- alarms generated on ports including the chassis type



Note — You do not have to set up separate policies, for example, VPLS, EPIPE, VPRN, services including the child object.

1 Perform one of the following to configure a policy from any configuration or object form:

   a Right-click on an NE, Shelf, Port, Daughter Card, or any other object to configure additional text policies. Choose Properties from the drop-down menu, the relevant form opens based on the object type.

   b Right-click on an alarm in the Alarm window, and choose View Alarmed Object. The relevant form opens based on the object type.

2 Click on the Additional Text Find icon at the bottom of the form. The Find Additional Text Attribute in (Edit) form opens.



Note — The Find Additional Text Attribute window lists all parameters on the property form including the parameters located on hidden tabs. If you need to temporarily display a tab, panel or field located on a hidden tab, click on the Show on Form button, the tab is temporarily added to the property form.

3 Choose an attribute from the list and click on the Create button. The Additional Text Attribute (Create) form opens.



Note 1 — You can search for any attributes using this option.

Note 2 — You can click on the Show on Form button to view the selected attribute in the list on the relevant form.

4 Select any or all of the following check boxes:

- Itself
- Its Children
- Its Association
- Its Peers

5 Click on the OK button to apply the changes. The Alarm Settings form opens with the Additional Text tab displayed and the newly configured policy highlighted.

6 Choose the newly configured additional text policy and perform one of the following:

   a Click on the Show Applicable Object Types to view Itself, Its Children, Its Association and Its Peers.

   b Click on the Properties button to configure the additional text attribute.

c Click on the Delete button to delete a selected additional text policy. A confirmation dialog box opens. Click on the Yes button to confirm the action.

d To check the attributes that appear in the Additional Text area of alarms raised on a particular object, paste the object identifier from the clipboard, (see Procedure 3-16 to copy a property form to the clipboard) and click on the Highlight Policies button, the relevant attributes are highlighted.

7 Click on the X icon to close the form.

Procedure 31-6 To set a policy to clear an alarm that is not implicitly cleared

1 In the dynamic alarm list, choose an alarm which is not checked in the Implicitly Cleared column and for which you want to set an alarm clearing policy. Perform one of the following:

a Double-click on the alarm. The Alarm Info form opens.

b Right-click on the alarm and choose Show Alarm(s) from the drop-down menu. The Alarm Info form opens.

2 Click on the View Policy button. The Specific Alarm Policy (Edit) form opens.

3 Configure the Auto Deletion Rule parameter.

4 Click on the OK button. A dialog box appears.

5 Click on the Yes button. The Alarm Info form is displayed.

6 Close the Alarm Info form.

Procedure 31-7 To configure alarm filters for OSS clients using the 5620 SAM GUI

Perform this procedure if required, to configure a filter to allow OSS clients to search for alarms using the 5620 SAM GUI. You can assign them an existing public alarm filter. See "Filtering alarms for OSS clients using the 5620 SAM GUI" in section 31.1 and the *5620 SAM XML OSS Interface Developer Guide* for more information.

This procedure presumes you have created an appropriate user account for the OSS client prior to starting this procedure. See "5620 SAM user security tasks" in the *5620 SAM System Administrator Guide* for information about how to create a 5620 SAM user account for OSS client users.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the Users tab.

3 Choose a user from the list, and click on the Properties button. The User (Edit) form opens.

4 Expand the OSS Session panel, if required.

5 Click on the Select button. The Select Public Alarm Filter for OSS-User form opens.

6 Perform one of the following:

a If required, click on the Search button to populate the list. Go to step 7.

b Create an alarm filter.

i Click on the Create button. The Create AlarmObject Filter form opens.

ii Configure an appropriate filter for the OSS client by selecting a filter from the Attribute parameter pull-down menu. You can modify the filter string to meet the operational requirements for an OSS client by configuring the Function, Value, and Operators pull-down menus as appropriate.

iii Click on the Add button to add the filter.

iv Repeat the above steps as required to add additional filter criteria for the alarm filter.

v Click on the Save button. The Save Filter form opens.

vi Configure the parameters:

- Filter Name
- Description
- Public



Note — The Public parameter must be enabled. Only public filters are applied to OSS clients.

vii Click on the Save button in the Save Filter form. The Save Filter form closes.

viii Click on the Clear button, if required, to remove an existing filter.

ix Close the Create AlarmObject filter form.

7 Choose a filter from the list, and click on the OK button. The Select Public Alarm Filter for OSS-User form closes, and the selected filter is applied.

8 Click on the OK button on the User (Edit) form. If an OSS connection exists for the user selected in step 3, a dialog box opens.

9 If required, click on the Yes button to close the dialog box. The User (Edit) form closes.

10 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 31-8 To reload all alarms from the historical alarm database

The 5620 SAM uses an alarm service to cache alarm information. To ensure the cache is current with all alarms stored in the historical alarm database, administrators can reload all alarms from the database. This procedure can only be performed by a user with an account that is assigned the administrator scope of command role or a scope of command role with write access permissions to the fm.FaultManager class, and should only be done when necessary.



Caution — After the procedure is complete, client GUI users viewing open alarm forms and windows may have out-of-date information. Operators should close all open windows and forms, then relaunch them. This includes windows and forms displaying alarm status information, for example, the navigation tree.

1 Log in to a 5620 SAM client GUI with a user account that is assigned the administrator scope of command role or a scope of command role with write access permissions to the fm.FaultManager class. Enter and confirm the password and click on the OK button.

2 Choose Administration→Reload Alarm Information from the 5620 SAM main menu.

3 Clicking on the OK button to confirm that you are aware of all of the other users that will be affected by the alarm reload.

Alarm information is reloaded, and all active client GUIs are updated with the confirmation message that the alarms have been reloaded. Client GUI users can close then reopen windows as required, to refresh the alarm information.

4 Click on the OK button to confirm the message.

5 Close then reopen any open windows or forms, if required.

Procedure 31-9 To enable or disable audible alarms

1 Choose Application→User Preferences from the 5620 SAM main menu. The User Preferences form opens with the General tab displayed.

2 Select the Turn on Audible Alarms check box in the Alarm Window panel.

3 Click on the OK button. The User Preferences form closes, and the audible alarm option is applied.

Procedure 31-10 To enable or disable the display of alarm flags in the alarm window

You can optionally display alarm flags in the alarm widow which appear on the Alarm Table tab. The flags displays the number of detected alarms since the flag was reset and are color-coded by severity. The time that the last alarm for that severity was detected is also displayed.

1 Choose Application→User Preferences from the 5620 SAM main menu. The User Preferences form opens with the General tab displayed.

2 Select the Show Alarm Flags check box in the Alarm Window panel. You can show or hide alarm flags.

3 Click on the OK button. The User Preferences form closes, and the Monitoring Flag panel appears in the dynamic alarm list alarm window.

Procedure 31-11 To enable or disable the display of correlated alarms in the alarm window

Note 1 — The display of correlated alarms may slow GUI performance when the 5620 SAM adds the alarms to the dynamic alarm list.

Note 2 — When you disable the display of correlated alarms in the dynamic alarm list, the correlated alarms are still listed in the Correlated Alarms tab on the Alarm Info form.

Note 3 — You can configure the Show Correlated Alarms parameter on a per-session basis. The display of correlated alarms is automatically updated by the Show Correlated Alarms by Default parameter when the 5620 SAM client application loads.

1 Enable or disable the default display of correlated alarms in the alarm window.

- **i** Choose Application→User Preferences from the 5620 SAM main menu. The User Preferences form opens with the General tab displayed.
- **ii** Configure the Show Correlated Alarms by Default parameter.
- **iii** Click on the OK button. The User Preferences form closes and the display of correlated alarms in the alarm window is updated.

2 Enable or disable the display of correlated alarms in the alarm window.

- **i** Choose Application→Alarm Window from the 5620 SAM main menu, if required. The alarm window is displayed.
- **ii** Configure the Show Correlated Alarms parameter. Correlated alarms are displayed in the alarm window.

Note — The Alarm Window titlebar displays Correlated Alarms Not Shown when correlated alarm display is disabled.

Procedure 31-12 To enable or disable the display of alarmed equipment in navigation trees for the View Alarmed Object function

When you apply the View Alarmed Object button or contextual menu option, the properties form for the alarmed object opens. Perform this procedure to configure an option to display the equipment navigation tree in the object properties form, for applicable equipment. When the option is enabled, the navigation tree is displayed in the properties form, with the alarmed equipment highlighted. The option applies to alarmed equipment under the Shelf level, such as card slots, ports, and channels. The option does not apply to logical groups, APS bundles, APS groups, fans and power supplies.

1 Choose Application→User Preferences from the 5620 SAM main menu. The User Preferences form opens with the General tab displayed.

2 Configure the parameter Enable properties forms with navigation trees when 'View Alarmed Object' button is applied.

3 Click on the OK button. A dialog box opens.

4 Click on the Yes button. The User Preferences form closes.

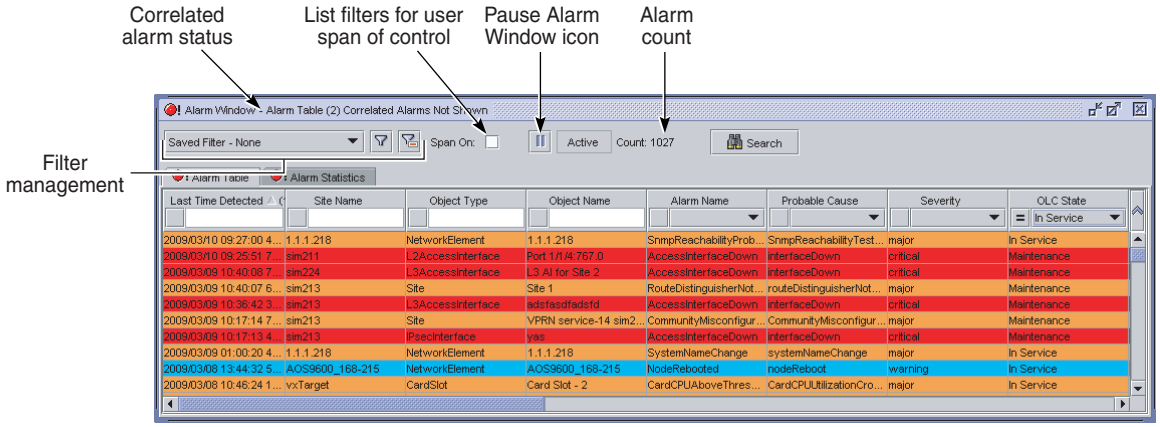
Procedure 31-13 To view and manage network alarms in the Alarm window

You can view the dynamic alarm list in the Alarm window to monitor incoming faults from all network objects and the 5620 SAM system. See Figure 31-10.

See chapter 3 for information about the following functions and features of the Alarm Window:

- Search filters
- Span On
- Equipment Groups
- Save to File
- Column heading searches
- Column heading contextual menu options

Figure 31-10 Dynamic alarm list Alarm Window



19623

1 Click on the Alarm Table tab in the Alarm Window. The dynamic list of incoming network alarms is displayed.

Note 1 — You can open up to six alarm windows, which allows you to view multiple filtered incoming network alarms.

Note 2 — You can pause the dynamic alarm list to prevent automatic scrolling when you view alarms. See Procedure 31-22.

2 Filter the alarms, if required.

Note — Sorting large numbers of alarms may slow GUI performance. Use filters to return a reasonable number of alarms. See Procedure 31-16 for information about creating search filters for network alarms.

3 Review the alarm information. See Table 31-1 for the types of information in an alarm. Scroll horizontally to view the information in the alarm.

Note 1 — Manage alarms according to your fault management policies. For information about troubleshooting using alarm information guidelines, see "Troubleshooting using network alarms" in the *5620 SAM Troubleshooting Guide*.

Note 2 — You can choose multiple alarms at the same time. When you choose multiple alarms, actions are performed on all selected alarms. Some actions open multiple forms, one for each alarm or object. See chapter 3 for more information about displaying multiple forms.

4 Right-click on an alarm and choose any of the following contextual menu options to manage an alarm:

a Choose Show Alarm(s) to open the Alarm Info form for the alarm. See Procedure 31-15 for more information about using the Alarm Info form to view and manage alarms.

b Choose View Alarmed Object to open the properties form for the object against which the alarm is raised. See Procedure 31-12 for information about displaying alarmed equipment in the properties form navigation tree when you choose View Alarmed Object.

c Choose Acknowledge Alarm(s). See Procedure 31-17.

d Choose Assign Severity. See Procedure 31-19.

e Choose Assign OLC State.

f Choose Delete Alarm(s) and click on the Yes button. You must have the appropriate span of control permissions to delete alarms.



Caution — You cannot recover a deleted alarm, unless the alarm is configured to be logged on deletion. See Procedure 31-2.



Note — You can delete an alarm only when the alarm settings are appropriately configured. See Procedure 31-1.

g Choose Clear Alarm(s) and click on the Yes button. The alarm is cleared from the list, and is added to the alarm log as an alarm history record, if so configured.



Note 1 — Self-clearing alarms are automatically cleared from the alarm list after the condition that triggered the alarm is no longer present. A check mark in the Implicitly Cleared field identifies self-clearing alarms.

Note 2 — You can set a policy to clear any alarm that is not implicitly cleared. See Procedure 31-6.

h Choose NE Sessions to open an SSH or Telnet session with the managed equipment that generated the alarm. See chapter 11. You can also open an FTP file browser. You must have the appropriate span of control permissions.

i Choose Show Sorting to manage the display of alarm information. See Procedure 3-30.

j Choose Copy to Clipboard. See Procedure 31-23.

k Choose View Alarm(s) History to open the Historical Alarms form. The filter is configured with the Alarm Name and Alarmed Object ID attributes equal to the Alarm Name and Alarmed Object ID of the alarm you are viewing. See Procedure 31-25.

l Choose View Object Alarm(s) History. See Procedure 31-26.

5 To view detailed information about a specific alarm, double-click on the alarm, or choose the alarm and click on the View Alarm button, to open the Alarm Info form. See Procedure 31-15 for more information about using the Alarm Info form to view and manage alarms.

Procedure 31-14 To view and manage object alarms on object properties forms

Network objects are displayed on the navigation tree and include equipment, logical components, and services. You can view and manage alarms raised against network objects for all NEs in the network down to the service, path, or port level. The 5620 SAM analyzes all incoming alarms to ensure that the alarms are listed against the appropriate equipment or service. This feature is useful when you troubleshoot an equipment or service problem.

Objects that can have alarms raised against them contain a Faults tab on their properties form. When you click on the Faults tab a list is displayed of the alarms raised against the specific equipment or service. When alarms are present, an indicator appears on the Faults tab. For some objects, the Faults tab contains subtabs for Object Alarms, Affecting Alarms, Aggregated Alarms, and Alarms on Related Objects. You can use these subtabs to display alarms raised against specific objects such as equipment, and associated objects such as services that use the equipment.

1 Perform one of the following to open the properties form for the required object:

a From the topology map:

Double-click on the object icon or right-click and choose Properties from the contextual menu. The properties form opens for the selected object.

b From the navigation tree:

i Navigate to the object.

ii Right-click on the object and choose Properties from the contextual menu. The properties form opens for the selected object.

c From the 5620 SAM main menu:

i Choose Manage→Equipment→Equipment. The Manage Equipment form opens. Alternatively, choose Manage→Service→Services for service-related objects. The Manage Services form opens.

ii Choose an object type from the Select Object Type drop-down menu. On the Manage Services form, the Service (Service Management) object type is displayed by default.

iii Configure the filter criteria, if required, and click on the Search button. A list of objects appears.

iv Choose an object from the list and click on the Properties button. The properties form opens for the selected object.

2 Click on the Faults tab.

3 Click on a subtab, if required. A list of object alarms appears.

4 Filter the alarms, as required.



Note — Sorting large numbers of alarms may slow GUI performance. Use filters to return a reasonable number of alarms. See Procedure 31-16.

5 Review the alarm information. See Table 31-1 for the types of information in an alarm. Scroll across each line to view the information in the alarm.



Note 1 — Manage alarms according to your fault management policies. For information about troubleshooting using alarm information guidelines, see "Troubleshooting using network alarms" in the *5620 SAM Troubleshooting Guide*.

Note 2 — You can choose multiple alarms at the same time. When you choose multiple alarms, actions are performed on all selected alarms. Some actions open multiple forms, one for each alarm or object. See chapter 3 for more information about displaying multiple forms.

6 To manage an alarm, right-click on the alarm and choose any of the following options from the contextual menu:

a Choose Show Alarm(s) to open the Alarm Info form for the alarm. See Procedure 31-15.

b Choose Acknowledge Alarm(s); see Procedure 31-17.

c Choose Assign Severity, see Procedure 31-19.

d Choose Delete Alarm(s) and click on the Yes button. You must have the appropriate span of control permissions to delete alarms.



Caution — You cannot recover a deleted alarm, unless the alarm is configured to be logged on deletion. See Procedure 31-2.



Note — You can only delete alarms when the alarm settings are appropriately configured. See Procedure 31-1.

e Choose Clear Alarm(s) and click on the Yes button. The alarm is cleared from the list, and is added to the alarm log as an alarm history record, if so configured.



Note 1 — Self-clearing alarms are automatically cleared from the alarm list after the condition that triggered the alarm is no longer present. A check mark in the Implicitly Cleared field identifies self-clearing alarms.

Note 2 — You can set a policy to clear any alarm that is not implicitly cleared. See Procedure 31-6.

f Choose View Alarm(s) History to open the Historical Alarms form. The filter is configured with the Alarm Name and Alarmed Object ID attributes equal to the Alarm Name and Alarmed Object ID of the alarm you are viewing. See Procedure 31-25.

g Choose View Object Alarm(s) History; see Procedure 31-26.

7 To view detailed information about a specific alarm, double-click on the alarm, or choose the alarm and click on the View Alarm button, to open the Alarm Info form. See Procedure 31-15 for more information about using the Alarm Info form to view and manage alarms.

8 Click on the View Alarm History button to open the Historical Alarms form for the alarmed object. The filter is configured with the Alarm Name and Alarmed Object ID attributes equal to the Alarm Name and Alarmed Object ID of the alarm you are viewing. See Procedure 31-25.

9 Close the object properties form.

Procedure 31-15 To view and manage alarms using the Alarm Info form

The Alarm Info form provides detailed information about an alarm, and contains options for managing alarms. See Figure 31-2. You can access the Alarm Info form from the Alarm Window dynamic alarm list or the Faults tab alarm list on an object properties form.

1 Perform one of the following to open the Alarm Info form:

   a From the Alarm Window dynamic alarm list:

      i Click on the Alarm Table tab, if required. The dynamic alarm list is displayed.

      ii Filter the list, as required. See Procedure 31-16 for information about creating search filters.

      iii Double-click on an alarm, or right-click and choose Show Alarm(s). The Alarm Info form opens with the Alarm tab and Info subtab displayed.

   b From the Faults tab of the object properties form.

      i Open the properties form for the required object.

      ii Click on the Faults tab.

      iii Click on a subtab, if required. A list of object alarms displays.

      iv Filter the list, as required. See Procedure 31-16 for more information about creating alarm filters.

      v Double-click on an alarm in the list, or right-click and choose Show Alarm(s). The Alarm Info form opens with the Alarm tab and Info subtab displayed.

2 Review the information on the Alarm tab. Click on a subtab to view the information on that subtab. See Table 31-1 for the types of information in an alarm. See step 3 f for information about the Acknowledgement subtab.



Note 1 — To quickly find specific alarm information, click on the Find button. See Procedure 3-27 for more information.

Note 2 — Manage alarms according to your fault management policies. For information about troubleshooting using alarm information guidelines, see "Troubleshooting using network alarms" in the *5620 SAM Troubleshooting Guide*.

3 Perform any of the following to manage the alarm:

   a Click on the Copy to Clipboard button to copy the alarm information to the clipboard. See Procedure 31-23.

   b Click on the View Alarmed Object button to view the alarmed object. The properties form opens for the object. See Procedure 31-12 for information about displaying alarmed equipment in the properties form navigation tree when you choose View Alarmed Object.

c Click on the View Correlating Alarm button to return to the Alarm Info form for the original correlating alarm, when you view Correlated Alarms. The View Correlating Alarm button is only active on Alarm Info forms for Correlated Alarms. See step 6.

d Click on the Delete button to delete the alarm. Click on the Yes button to confirm the action, and then click on the OK button. You must have the appropriate span of control permissions to delete alarms.



Caution — You cannot recover a deleted alarm, unless deleted alarms are configured to be logged in the alarm history database. See Procedure 31-2.

e Click on the Clear button to clear the alarm. Click on the Yes button to confirm the action, and then click on the OK button. The alarm is cleared from the list, and is added to the alarm log as an alarm history record, if so configured.



Note 1 — Self-clearing alarms are automatically cleared from the alarm list after the condition that triggered the alarm is no longer present. A check mark in the Implicitly Cleared field identifies self-clearing alarms.

Note 2 — You can set a policy to clear any alarm that is not implicitly cleared. See Procedure 31-6.

f Click on the Acknowledge button to acknowledge the alarm. The Acknowledgement subtab opens, with the Notes subtab displayed. See Procedure 31-18.

g Click on the View Policy button. The Specific Policy form opens for the alarm. See Procedure 31-3.

h Click on the View Alarm History button to view the alarm history for the alarm. The Historical Alarms form opens. The filter is configured with the Alarm Name and Alarmed Object ID attributes equal to the Alarm Name and Alarmed Object ID of the alarm that you are viewing. See Procedure 31-25.

4 View affected objects, as required.

i Click on the Affected Objects tab.

ii Click on the Search button, if required.

iii Choose an object in the list and double-click or click on the Properties button. The properties form opens for the selected object.

5 View affecting objects, as required.

i Click on the Affecting Objects tab.

ii Click on the Search button, if required.

iii Choose an object in the list and double-click or click on the Properties button. The properties form opens for the selected object.

6 View and manage correlated alarms, as required.

i Click on the Correlated Alarms tab. The list of correlated alarms appears.

ii Filter the alarms, as required. See Procedure 31-16 for more information about creating search filters.

iii Choose an alarm in the list and double-click or click on the Properties button. The Alarm Info form for the correlated alarm opens. Alternatively, you can right-click on an alarm and choose an option from the contextual menu, as described in Procedure 31-14.

iv Manage the correlated alarm.

v If required, click on the View Correlating Alarm button to return to the Alarm Info form for the original correlating alarm.

7 Close the Alarm Info form.

Procedure 31-16 To create search filters to view specific network alarms

You can create and select filters to locate and view specific network alarms in the dynamic alarm list. You can save multiple filters and view the alarm information by opening up to 6 alarm windows. The name of the filter appears in the alarm window title of each alarm window that is open. Viewing network alarms using the dynamic alarm list is described in Procedure 31-13. Figure 31-10 shows the location of the Manage Filters icon in the alarm window.



Note — The FDN extension of a GNE alarm is not appended to the Alarm Name field in the 5620 SAM GUI, but is included in the Additional Text field. To create a filter for GNE alarms that have FDN extensions, you must filter on the Additional Text field.

1 Choose Application→Alarm Window. The Alarm Window opens.

2 Click on the Filter icon beside the filter drop-down list. The Alarm Window filter form opens.

3 Configure the filter criteria. See chapter 3 for more information.

4 Click on the Add button.

5 Click on the Save button. The Save Filter form opens.

6 Configure the parameters:

- Filter Name
- Description
- Public

7 Click on the Save button. The Save Filter form closes and the Alarm Window filter form reappears.

8 Click on Apply to apply the changes and close the Alarm Window filter form.

9 Click on the filter drop-down list. The saved filter is shown in the list.

10 Click on the saved filter to load and view the results of the filtered search in the dynamic alarm list. The number of alarms associated with the selected search filter appears in the Count field, as shown in Figure 31-10.

Procedure 31-17 To acknowledge alarms using the contextual menu on alarm lists

You can acknowledge alarms using the Alarm Acknowledgement form or the Acknowledgement subtab on the Alarm Info form. The Alarm Info form provides more options for alarm notes. See Procedure 31-18 for information about acknowledging alarms using the Alarm Info form.

Perform this procedure to acknowledge alarms, enter notes, and to change the urgency and severity of alarms. Alarms can be acknowledged multiple times.

Only operators with the appropriate span of control permissions can change the severity of alarms, when alarm settings are configured appropriately. See Procedure 31-1 for more information about alarm settings.

1 Perform one of the following to open the Alarm Acknowledgement form:

- **a** From the dynamic alarm list:
  - **i** Click on the Alarm Table tab in the Alarm Window, if required. The dynamic alarm list appears.
  - **ii** Filter the alarms, as required. See Procedure 31-16 for more information about creating search filters.
  - **iii** Right-click on an alarm in the list and choose Acknowledge Alarm(s) from the contextual menu. The Alarm Acknowledgement form opens and displays the selected alarm(s).
- **b** From the object properties form:
  - **i** Open the properties form for the required object. See Procedure 31-14.
  - **ii** Click on the Faults tab.
  - **iii** Click on a subtab, if required. A list of object alarms appears.

iv Filter the alarms, as required. See Procedure 31-16 for more information about creating search filters.

v Right-click on an alarm in the list and choose Acknowledge Alarm(s) from the contextual menu. The Alarm Acknowledgement form opens and displays the selected alarm(s).



Note — You can choose multiple alarms at the same time. Multiple alarms are all acknowledged with one action.

2 Enable and configure the parameters:

- Urgency
- Assigned Severity

3 When you acknowledge an alarm for the first time, ensure that the Acknowledgement parameter is enabled. When you disable the parameter, the alarm is not acknowledged. Changes to the Urgency and Assigned Severity parameters take effect even when the alarm is not acknowledged.

4 Click on the Acknowledgement Text field and enter any notes, as required.



Note 1 — You can enter notes up to 4000 characters or bytes (multibyte characters are supported), whichever limit is reached first.

Note 2 — Before you close the form, you can click on the Reset button to restore the original Urgency, Severity, and Acknowledgement settings.

Note 3 — Alarms can be acknowledged more than once. Notes can be entered each time that an alarm is acknowledged. You can view and revise notes, and view revision histories for notes using the Alarm Info form. See Procedure 31-18.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Alarm Acknowledgement form closes.

Procedure 31-18 To acknowledge alarms using the Alarm Info form

You can acknowledge alarms using the Acknowledgement subtab on the Alarm Info form or the contextual menus on alarm lists. The Alarm Info form provides more options for alarm notes. See Procedure 31-17 for more information about acknowledging alarms using the contextual menus.

Perform this procedure to acknowledge alarms, to change the urgency and severity of alarms, and to enter and revise alarm notes. You can also view the revision history of alarm notes. Alarms can be acknowledged multiple times.

Only operators with the appropriate span of control permissions can change the severity of alarms, when alarm settings are configured appropriately. See Procedure 31-1 for more information about alarm settings.

1 Open the Acknowledgement subtab on the Alarm Info form. See Procedure 31-15.

2 If you opened the Acknowledgement subtab by clicking on the Acknowledge button on the Info subtab, go to step 6.

3 Click on the Notes subtab, if required.

4 Click on the New button.

5 Click on the Note subtab in the lower half of the form, if required.

6 Configure the parameters, as required:

- Urgency
- Assigned Severity

7 When you acknowledge an alarm for the first time, ensure that the Acknowledgement parameter is enabled. When you disable the parameter, the alarm is not acknowledged. Changes to the Urgency and Assigned Severity parameters take effect even when the alarm is not acknowledged.

8 Perform one of the following to enter a note, or to view and revise notes for the alarm, as required:



Note 1 — You can enter notes up to 4000 characters or bytes (multibyte characters are supported), whichever limit is reached first.

Note 2 — You can view or revise existing notes from the list in the upper half of the Notes subtab. See chapter 3 for information about searching, sorting, and displaying lists.

a Enter a new note. Click in the Note field and enter the note text.

b View or revise an existing note.

i Choose a note in the Notes list in the upper half of the form, and click on the Properties button. The note displays in the Note field in the lower half of the form.

ii Configure the parameters, as required:

- Reason for Change
- Detailed Text

iii Revise the note, if required.

iv Click on the Revision History tab to view the revision history for the selected note, if required.



Note 1 — Before you close the form, you can click on the Reset button to restore the original Urgency, Severity, Note and Acknowledgement settings.

Note 2 — You can acknowledge alarms more than once. You can enter or revise notes each time that an alarm is acknowledged. New notes appear in the Notes list. When you apply a new note, the alarm is re-acknowledged. When you revise an existing note, the alarm is not re-acknowledged.

9 Click on the Note subtab and perform one of the following:

a Click on the Apply button to acknowledge the alarm.

b Click on the OK button to acknowledge the alarm and close the Alarm Info form.

Procedure 31-19 To manually promote or demote the severity of an alarm

Operators with the appropriate span of control permissions can change the severity of alarms when alarm settings are configured appropriately. See Procedure 31-1 for more information about configuring global alarm settings.

1 Perform one of the following to open the Severity Assignment form:

a From the dynamic alarm list:

i Click on the Alarm Table tab in the Alarm Window, if required.

ii Filter the alarms, as required. See chapter 3 for more information about creating search filters.

iii Right-click on an alarm in the list and choose Assign Severity from the contextual menu. The Severity Assignment form opens and displays the selected alarm(s).

b From the alarm list on the Faults tab of the object properties form:

i Open the object properties form for the required object. See Procedure 31-14.

ii Click on the Faults tab.

iii Click on a subtab, if required. A list of object alarms appears.

iv Filter the alarms, as required. See Procedure 31-16 for more information about creating alarm filters.

v Right-click on an alarm in the list and choose Assign Severity from the contextual menu. The Severity Assignment form opens and displays the selected alarm(s).



Note 1 — You can choose multiple alarms at the same time. When you choose multiple alarms, the new severity level is applied to all selected alarms.

Note 2 — You can also change the severity of an alarm using the Alarm Acknowledgement form or the Acknowledgement tab on the Alarm Info form. See Procedures 31-17 and 31-18.

2 Configure the Assigned Severity parameter.



Note — Before you close the form, you can click on the Reset button to restore the original severity setting.

3 Click on the OK button. A dialog box appears.

4 Click on the Yes button. The Severity Assignment window closes.

Procedure 31-20 To list alarms received during a specified time period

Perform this procedure to list the current and historical alarms for a specific time period. This consolidated view of all relevant alarms is useful for troubleshooting.

1 Click on the Alarm Table tab in the Alarm Window. The dynamic alarm list appears.

2 Choose one or more alarms in the list.

3 Click on the More Actions button and choose Current and Historical Alarms Snapshot. The Current and Historical Alarms Snapshot form opens, displaying current and historical alarms for the time period specified by the First Time Detected (minus buffer time) and Last Time Detected (plus buffer time) of the selected alarms.

4 If required, configure the Display Buffer Time (minutes) parameter.

5 Double-click on an alarm in the list to view alarm information. See Procedure 31-15.

6 Close the Current and Historical Alarms Snapshot form.

Procedure 31-21 To search for alarms received during a specified time period

Perform this procedure to search for historical alarms received during a specified time period.

1 Perform one of the following to search for historical alarms:

   a Choose Tools→Historical Alarms from the 5620 SAM main menu. The Historical Alarms form opens.

   b Choose More Actions→Historical Alarms from the Alarm Window. The Historical Alarms form opens.

2 Configure the Search for Alarms parameter.

3 Click on the Search button. A list of historical alarms is displayed, and the Oldest Alarm Searched and Oldest Alarm in Database fields are updated.



Note — Up to 500 000 alarms are displayed in the list. If the number exceeds 500 000, an error message is displayed.

4 Perform one of the following to view alarm information:

   a Double-click on an alarm in the list. The AlarmHistoryObject form opens.

   b Choose an alarm from the list and click on the Properties button. The AlarmHistoryObject form opens.

5 Click on the Cancel button to close the AlarmHistoryObject form. The Historical Alarms form is displayed.

6 Click on the View Alarmed Object button. The Properties form for the object, against which the historical alarm was raised, opens.

7 Close the Historical Alarms form.

Procedure 31-22 To pause the dynamic alarm list from scrolling when viewing alarms

Incoming alarms are added to the dynamic alarm list, with the most recent alarm shown first. Incoming alarms may cause the alarm list to scroll automatically. You can pause the dynamic alarm list to stop scrolling. Figure 31-10 shows the location of the Pause Alarm Window icon in the Alarm Window.

1 View alarms from the dynamic alarm list, as described in Procedure 31-13.

2 Click on the Pause Alarm Window icon. The icon changes to indicate that the dynamic alarm list Alarm Window is locked for viewing. The icon box changes to red and the text changes to Paused.

Incoming alarms are not added for the duration of the pause.

3 Click on the Start Auto-Update icon to unlock the dynamic alarm list Alarm Window. The icon changes to indicate the dynamic alarm list Alarm Window is active. The icon box changes to gray and the text changes to Active. Any alarms that occurred during the pause appear in the dynamic alarm list.



Note — You can also scroll lock the dynamic alarm list by highlighting a specific alarm. Incoming alarms appear above the selected alarm and the selected alarm continues to be selected in the dynamic alarm list. Scroll down to find the selected alarm.

Procedure 31-23 To copy alarm information to the clipboard

You can copy alarm information to the local clipboard buffer and then paste the information in other applications. This function allows you to share the alarm information for troubleshooting purposes.

1 Perform one of the following:

- **a** Copy from an Alarm Info form.
  - **i** Open the Alarm Info form for an alarm. See Procedure 31-15.
  - **ii** Click on the Copy to Clipboard button. The information for the alarm is copied to the clipboard.
- **b** Copy from the Alarm Window.
  - **i** Click on the Alarm Table tab, if required.
  - **ii** Right-click on an alarm in the dynamic alarm list, and choose Copy to Clipboard from the contextual menu. The information for the selected alarm is copied to the clipboard.

2 Paste the information in an application, as required.

Procedure 31-24 To view network alarm statistics

You can view alarm statistics using the Alarm Statistics table in the Alarm Window. The table provides a consolidated view of all alarms by severity and acknowledgement status.

1 Click on the Alarm Statistics tab in the Alarm window. The Alarm Statistics table displays the following information:

- number of acknowledged and unacknowledged alarms for each severity type
- total number of alarms of each severity type
- total number of acknowledged and unacknowledged alarms
- total number of alarms

2 View the alarm statistics information.

Procedure 31-25 To review historical alarm records

Alarms are logged as historical alarm records in an alarm log database.

1 Perform one of the following to review historical alarm records:

a Choose Tools→Historical Alarms from the 5620 SAM main menu. The Historical Alarms form opens.

b Choose More Actions→Historical Alarms from the Alarm Window. The Historical Alarms form opens.

2 If required, specify a filter to narrow the range of historical alarms displayed.



Note 1 — Sorting large numbers of alarms may slow GUI performance. Use filters to return a reasonable number of alarms. See Procedure 31-16 for more information about creating search filters.

Note 2 — The Historical Alarm form displays the Total Number of Alarms in Database, the Oldest Alarm Searched and the Oldest Alarm in Database.

3 Click on the Search button. The list of historical alarm records appears based on the filtering criteria.

4 Choose a historical alarm record from the list.

5 Click on the Properties button to review the alarm. The AlarmHistoryObject form appears.

Table 31-1 lists the information displayed for each historical alarm record. Table 31-4 lists the additional historical alarm information available from the Historical Alarms form for logged alarms.

Table 31-4 Alarm information from the Alarm History Object form

Alarm field	Information
Info tab on Alarm History Object form	
Alarm Status	Reason the alarm was logged to the historical alarm database
Time Logged	Timestamp when the alarm was moved to the historical alarm database

6 Click on the Cancel button to close the AlarmHistoryObject form. The Historical Alarms form is displayed.

7 Choose the View Policy button from the Historical Alarms form to view the Specific Policy form to manage the logged historical alarm records. See Procedure 31-3 for more information.



Caution — You cannot recover alarms purged from the historical alarm database log. If you want to save information about those alarms, save a file containing the alarm history database log details, as described in Procedure 31-27.

8 Close the Historical Alarms form.



Note — When the maximum number of alarms allowed in the alarm log is reached, the oldest alarms are deleted. If you want to save information about those alarms, save a file containing the alarm log details, as described in Procedure 31-27.

Procedure 31-26 To view the source object of an historical alarm

1 Choose one of the following to view the object that was the source of the alarm:

- **a** Choose Tools→Historical Alarms from the 5620 SAM main menu. The Historical Alarms form opens.
- **b** Choose More Actions→Historical Alarms from the Alarm Window. The Historical Alarms form opens.

2 As required, choose a filter to narrow the range of historical alarms displayed.

3 Click on the Search button. The historical alarm records appear based on the filter.

4 Choose an alarm record from the list, and click on the Properties button to view the alarm. The AlarmHistoryObject form appears.

5 Click on the View Alarmed Object button. The properties form opens for the object against which the historical alarm record was raised.

Procedure 31-27 To save lists of logged historical alarm records

1 Perform one of the following:

   a Choose Tools→Historical Alarms from the 5620 SAM main menu. The Historical Alarms form opens.

   b Choose More Actions→Historical Alarms from the Alarm Window. The Historical Alarms form opens.

2 If required, choose a filter to narrow the range of historical alarms displayed.

3 Click on the Search button. The list of logged historical alarm records appears.

4 Sort the list of logged historical alarm records, as required.

5 Right-click on a list column heading and choose Save To File from the contextual menu. The Save As form opens.

   i Choose a directory to save the listed information using Save In

   ii Create a filename of any length using File Name

   iii Choose a format for the output file using Files of Type: HTML or comma-delimited CSV

6 Click on the Save button. The information is saved in the appropriate file format.

7 Close the Historical Alarms form.

32 — OAM diagnostic tests

32.1 OAM diagnostic tests overview *32-2*

32.2 Sample OAM diagnostic test configuration *32-22*

32.3 Workflow to use OAM diagnostic tests *32-24*

32.4 OSS OAM Test Results file retrieval *32-26*

32.5 OAM diagnostic tests procedures *32-26*

32.1 OAM diagnostic tests overview

The proper delivery of services requires that a number of operations must occur correctly at different levels in the service. For example, operations such as the association of packets to a service, VC labels to a service, and each service to a service tunnel, must be performed successfully for the service to pass traffic to subscribers according to SLAs.

Even when tunnels are operating correctly and are correctly bound to services, incorrect information may cause connectivity issues.

To verify that a service is operational and that configuration information is correct, a set of configurable in-band or out-of-band, packet-based OAM tools is available.

For in-band, packet-based testing, the OAM packets closely resemble customer packets to effectively test the forwarding path. However, these packets are distinguishable from customer packets, so they are kept within the service provider network and not forwarded to the customer. For out-of-band testing, OAM packets are sent across a portion of the transport network, for example, across LSPs to test reachability.

You can configure and manage OAM tests:

- from the properties forms of network objects, for example, LSP pings from the LSP properties form
- from the Manage Tests form
- from the service and composite service flat topology maps

You can create and schedule the execution of test suites that contain groups of OAM tests using the 5620 SAM Service Test Manager, or STM. See chapter 77 for information about the STM. See chapter 7 for information about scheduled tasks. See chapter 6 for information about managing tests and test results using service flat topology maps.



Note — If you attempt to modify an OAM test or test suite that is deployed to a suspended NE, the 5620 SAM raises an alarm. The alarm does not automatically clear when the NE is remanaged.

Table 32-1 lists the supported OAM test types, the objects against which the tests can be performed, the test types, and the network layer being tested.

Table 32-1 OAM test types and test objects

Network level	Test type	Network object or service component for test
Application (level 7)	DNS lookup	DNS
	DHCP lookup (1)	DHCP

(1 of 3)

Network level	Test type	Network object or service component for test
Ethernet	CFM Loopback	Ports
	CFM Global MEG	
	CFM Link trace	
	CFM Continuity Check	
	CFM One Way Delay	
	CFM Two Way Delay	
	CFM Eth test	
	CFM Single Ended Loss	
	CFM Two Way Synthetic Loss Measurement (SLM)	
Service (level 6)	VPRN ping	VPRN site
	VPRN trace	
	ICMP ping	
	ICMP trace	
	CPE ping	VPLS site Epipe VLL site
	MFIB ping	
	ANCP loopback	Network element
	VCCV ping	VLL
	VCCV trace	VLL
	MAC populate	VPLS site Epipe VLL site VLL
	MAC ping	
	MAC trace	
	MAC purge	
Service transport binding (level 5)	Service site ping	Network element
Service transport (level 4)	MTU ping	Service tunnel (SDP)
	SDP ping	
Transport (level 3)	LSP ping	LSP LSP path MPLS-TP LSP
	LSP trace	
	P2MP LSP ping	P2MP LSP, P2MP mLDP P2MP path
	P2MP LSP trace	
	LDP ping (1)	MPLS site LDP site
	LDP trace (1)	
	LDP tree trace	

(2 of 3)

Network level	Test type	Network object or service component for test
Routed network (level 2)	ICMP ping	IP unicast traffic
	ICMP traceroute	
	OmniSwitch ping and traceroute(3)	
	Multicast trace	IP multicast traffic
	Multicast stat (2)	
	Multicast router information	
Layer 1 or Layer 2 (level 1)	MAC ping (2)	Ethernet
	MAC traceroute (2)	
	ATM ping	ATM PVC connection

(3 of 3)

Notes

(1) Cannot be performed using the 5620 SAM or using CLI on devices.

(2) Not yet supported using the 5620 SAM but is supported using CLI on devices.

(3) Implemented using user-defined scripts

Ethernet CFM

Ethernet Connectivity Fault Management (CFM) supports end-to-end service management in an L2 network. CFM tools provide path discovery and fault detection, isolation, and notification. See chapter 78 for more information about how to configure an IEEE 802.1ag-enabled network for Ethernet CFM.

The following CFM diagnostic tests detect connectivity failure.

CFM continuity check

CFM continuity check, or CC, messages, are multicast messages that a MEP transmits periodically to remote MEPs in the same MEG. CC tests are used to discover a remote end point, check the health of a site, and detect cross-connect misconfigurations. The loss of three consecutive CCM messages, or the receipt of a CCM with incorrect information, indicates a fault.



Note 1 — If a service is modified after you associate it with an MD, for example, a new site is added, you must manually add new MEPs, as required.

Note 2 — If a CFM continuity check test is running on a service when you add a new MEP to the service, you must stop the test and execute it again to make the new MEP active.

Note 3 — When a service is modified after a CFM continuity check is created, for example, a new B-VPLS site is added to the service, you must manually add a virtual MEP to the site.

CFM dual-ended loss

A CFM dual-ended loss test functions as an optional extension of a CC test. It applies only to Y.1731 MEPs. This type of test is used to calculate the rate of frame loss in each direction for Ethernet packets sent between two MEPs. When a CC test is executed with the dual-ended loss option enabled, the option is replicated on all participating MEPs that support the test, along with the accompanying alarm threshold values. If a MEP detects that the local or remote frame loss ratio has exceeded the alarm threshold for a remote MEP, the MEP raises an alarm against the remote MEP.

CFM single-ended loss

The CFM single-ended loss test applies only to Y.1731 MEPs. This one-way test originates on a source MEP and terminates on a destination MEP. The target of a single-ended loss test is a destination MAC address. The test is used to calculate the rate of frame loss in each direction for Ethernet packets sent between the two MEPs.

CFM loopback

CFM loopback messages are sent to a unicast destination MAC address. The MEP at the destination responds to the loopback message with a loopback reply. A MEP or a MIP can reply to a loopback message if the destination MAC address matches the MAC address of the MEP or MIP. CFM loopback tests verify connectivity to a specific MEP or MIP.

CFM link trace

CFM link trace messages that contain a target unicast MAC address are sent to multicast destination MAC addresses. Each MIP at the same MD level replies with a link trace response. Messages are forwarded to the next hop until they reach the destination MAC address. The originating MEP collects the replies to determine the path.

CFM one-way delay

The CFM one-way delay test applies only to Y.1731 MEPs. The test originates on one MEP and terminates on a target MEP. The results are read from the target MEP. In the test, frame delay is defined as the time elapsed since the start of transmission of the first bit of the frame by a source site until the frame is received by the destination site. The frame delay represents the one-way trip time between the source and destination sites.

CFM two-way delay

The CFM two-way delay test applies only to Y.1731 MEPs. In this test, the frame delay is defined as the time elapsed since the start of transmission of the first bit of the frame by the source site until the frame is received by the same site after passing through the destination site. The frame delay represents the round-trip time between the source and destination sites.

CFM Eth

The CFM Eth test applies only to Y.1731 MEPs. This one-way test originates on a source MEP and terminates on a destination MEP. The target of a CFM Eth test is a MAC address. The test is used to perform one-way in-service diagnostics that include verifying bandwidth throughput, frame loss, and bit errors. To perform the test, a MEP inserts frames with Eth-test information that includes specific throughput, frame size, and transmission patterns. A MIP is transparent to Eth-test frames.

CFM two-way SLM

The CFM two-way SLM test provides Synthetic Loss Measurement and is used to check packet loss.

Note — On the 7705 SAR, SLM is only supported on Epipe services under the following conditions:

- single-ended (two-way) loss measurement using optional TLV with a timestamp on the near-end and far-end for combined loss and delay measurement
- unicast destination addresses only
- DOWN MEP direction for Spoke-SDPs only (UP and DOWN MEP direction for SAPs)

MTU ping OAM

The MTU Ping OAM diagnostic tool, which is called sdp-mtu in the CLI, provides a tool for service providers to determine the exact frame (MTU) size that is supported on a service tunnel (also called an SDP), to within one byte. Use the MTU ping OAM to:

- determine the maximum frame size supported between the service ingress and the service termination point
- solve troubleshooting issues that are related to equipment used across the network core that may not be able to handle large frame sizes

In a large network, network devices can support a variety of packet sizes, up to a limit, that are transmitted across its interfaces. This size limit is referred to as the MTU of network interfaces. You must consider the MTU of the entire service tunnel end-to-end when you provision services, especially for VLL services in which the service must support the ability to transmit the largest customer packet.

Note — The OAM messages which operate over an LDP LSP, and/or over a PW signalled by T-LDP, and which require a response using the IP path, must use a source IP address which is reachable within the same routing domain as that of the LSR ID of the LDP or T-LDP session. The messages of the MTU Ping OAM tool use the T-LDP local LSR ID as the source IP address. Previously the NE's system interface address was used for this purpose.

Tunnel ping OAM

The Tunnel Ping OAM tool, which is called sdp-ping in the CLI, performs in-band unidirectional or bidirectional connectivity tests on service tunnels (also called an SDP). The OAM packets are sent in-band in the tunnel encapsulation, so they follow the same path as the service traffic. The response can be received out-of-band in the control plane or in-band using the data plane for a bidirectional test.

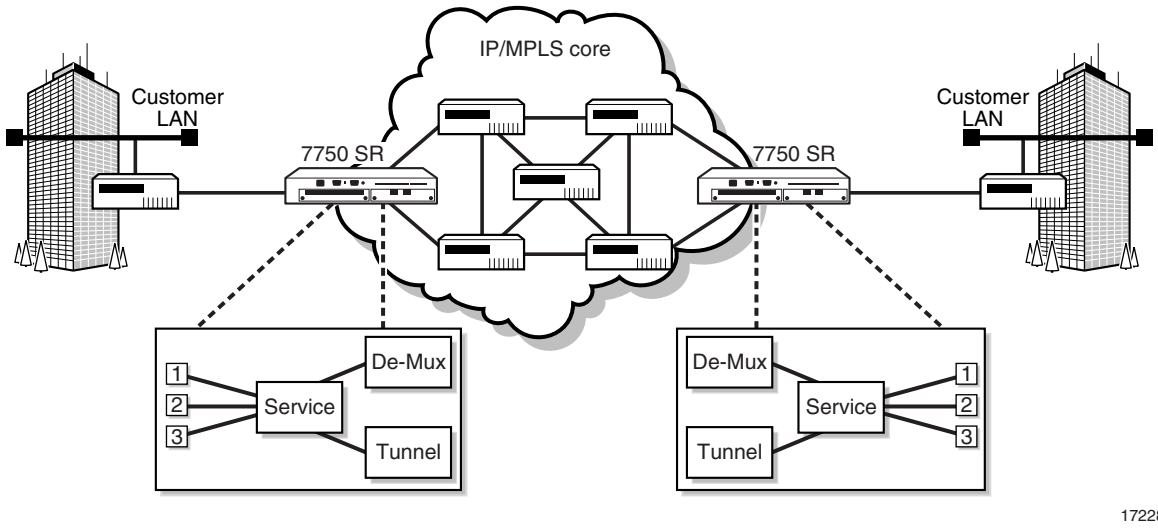
For a unidirectional test, tunnel ping OAM tests:

- egress service tunnel ID encapsulation
- whether the packet can reach the far-end IP address destination of the service tunnel ID within its encapsulation
- whether a packet of the specified size goes to the far-end IP address of the service tunnel ID within its encapsulation
- forwarding class mapping to ensure that the test packet is treated the same as the customer traffic
- determine whether SLA delay metrics are met

For a bidirectional test, tunnel OAM uses a local egress service tunnel ID and an expected remote service tunnel ID, so the user can specify where the returned messages should be sent from based on the far-end tunnel ID.

Figure 32-1 shows how a tunnel OAM packet can be inserted to test the connectivity between two customer LANs across the IP/MPLS core.

Figure 32-1 Sample OAM diagnostic



Note — The OAM messages which operate over an LDP LSP, and/or over a PW signalled by T-LDP, and which require a response using the IP path, must use a source IP address which is reachable within the same routing domain as that of the LSR ID of the LDP or T-LDP session. The messages of the Tunnel Ping OAM tool use the T-LDP local LSR ID as the source IP address. Previously the NE's system interface address was used for this purpose.

Service site ping OAM

The Service Site Ping OAM diagnostic tool, which is called svc-ping in the CLI and was formerly called the circuit ping, provides end-to-end connectivity testing for an individual service. This diagnostic operates at a higher level than the tunnel OAM ping because it verifies connectivity for an individual service rather than connectivity across the service tunnel. This allows you to isolate a problem within the service rather than at the port, which is the endpoint of the service tunnel.

The diagnostic tests a service ID for correct and consistent provisioning between two service endpoints. The following information can be obtained from a service site ping OAM:

- verification that the local and remote service sites exists
- verification of the current state of the local and remote service sites
- ensuring that the local and remote service types are correlated
- ensuring that the same customer is associated with the local and remote service sites
- ensuring that there is a service-to-circuit association at both the local and remote service sites using the Use Local Tunnel and Use Remote Tunnel options, to check the circuit between service sites
- verification that the local and remote ingress and egress service labels match



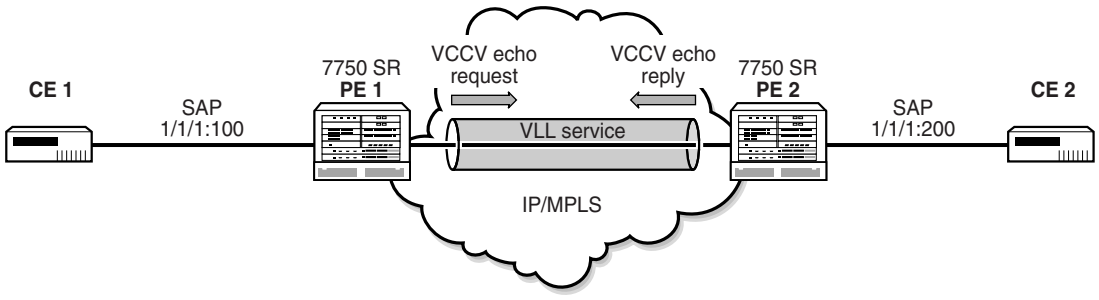
Note — The OAM messages which operate over an LDP LSP, and/or over a PW signalled by T-LDP, and which require a response using the IP path, must use a source IP address which is reachable within the same routing domain as that of the LSR ID of the LDP or T-LDP session. The messages of the Service Site Ping OAM tool use the T-LDP local LSR ID as the source IP address. Previously the NE's system interface address was used for this purpose.

VCCV Ping OAM

The VCCV Ping OAM diagnostic tool, which is called vccv-ping in the CLI, performs in-band connectivity tests. It can be used for VPLS, MVPLS, HVPLS, and all types of VLLs.

When applied to a VLL service, the test supports cross-circuit tests as long as the circuit types match; for example, an Epipe-to-Epipe connector, or an Epipe-to-VPLS/MVPLS site connector. The purpose of the ping is to determine that the destination PE device is the egress for the L2 FEC. Figure 32-2 shows a VCCV Ping.

Figure 32-2 VCCV Ping OAM diagnostic



In this example, the ping test packet or packets are sent with the destination IP address of PE 2. The request is encapsulated in a VLL packet and is forwarded to PE 2. PE 2 replies to the source device IP address. The packets are sent using the same encapsulation and along the same path as user packets in the VLL. This test provides a check of both the control plane and the data plane.

Note — The OAM messages which operate over an LDP LSP, and/or over a PW signalled by T-LDP, and which require a response using the IP path, must use a source IP address which is reachable within the same routing domain as that of the LSR ID of the LDP or T-LDP session. The messages of the VCCV Ping OAM tool use the T-LDP local LSR ID as the source IP address. Previously the NE's system interface address was used for this purpose.

When this test is applied to a VPLS, MVPLS or HVPLS, downstream SDP bindings are not configurable as they are in VLL services. Downstream bindings are typically related to switching sites and these are not relevant to VPLS. In VPLS, only the first SDP binding is configured, and this can be either a mesh or spoke binding.

In addition, since an HVPLS comprises a mixture of active and standby spokes, the VCCV Ping test execution will only be successful on active spokes that have associated active return spokes. A test suite will generate all the required VCCV Ping tests, but only active spokes with active return spokes are counted in the statistics results. This also includes any service connector used in a composite service, provided that the connector is a spoke connector between a VPLS and an Epipe service.

VCCV trace OAM

The VCCV Trace OAM diagnostic tool, which is called vccv-trace in the CLI, displays the hop-by-hop path used by a VLL. VCCV trace can trace the entire path of a PW with a single command issued at the T-PE or at an S-PE. It is an iterative process by which the ingress T-PE or T-PE sends successive VCCV-Ping messages with incrementing the TTL value, starting from TTL=1. The process is terminated when the reply is from the egress T-PE or when a timeout occurs.

Note — The OAM messages which operate over an LDP LSP, and/or over a PW signalled by T-LDP, and which require a response using the IP path, must use a source IP address which is reachable within the same routing domain as that of the LSR ID of the LDP or T-LDP session. The messages of the VCCV Trace OAM tool use the T-LDP local LSR ID as the source IP address. Previously the NE's system interface address was used for this purpose.

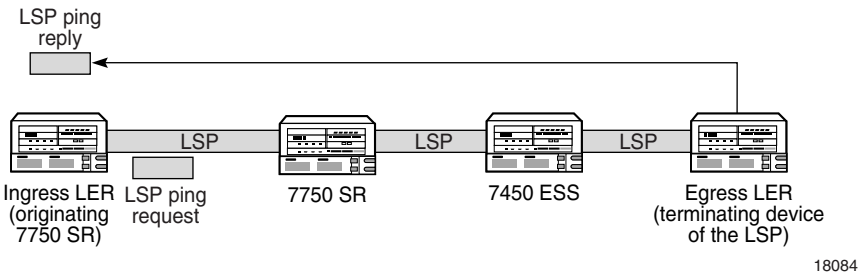
LSP Ping OAM

The LSP Ping OAM diagnostic tool, which is called lsp-ping in CLI, performs in-band LSP and MPLS-TP LSP connectivity tests. The following information can be determined from the test:

- detect data plane failures in LSPs or MPLS-TP LSP and with LSP or MPLS-TP LSP connectivity
- test whether the LSP or MPLS-TP LSP tunnels are working in both directions

In an LSP or MPLS-TP LSP ping, the originating router creates an MPLS echo request packet for the LSP and MPLS path to be tested. The MPLS echo request packet is sent and awaits an MPLS echo reply packet from the router that terminates the LSP. The status of the LSP is displayed when the MPLS echo reply packet is received. Figure 32-3 shows an LSP ping.

Figure 32-3 LSP Ping diagnostic



Note — The OAM messages which operate over an LDP LSP, and/or over a PW signalled by T-LDP, and which require a response using the IP path, must use a source IP address which is reachable within the same routing domain as that of the LSR ID of the LDP or T-LDP session. The messages of the LSP Ping use the T-LDP local LSR ID as the source IP address. Previously the NE's system interface address was used for this purpose.

LSP Trace OAM

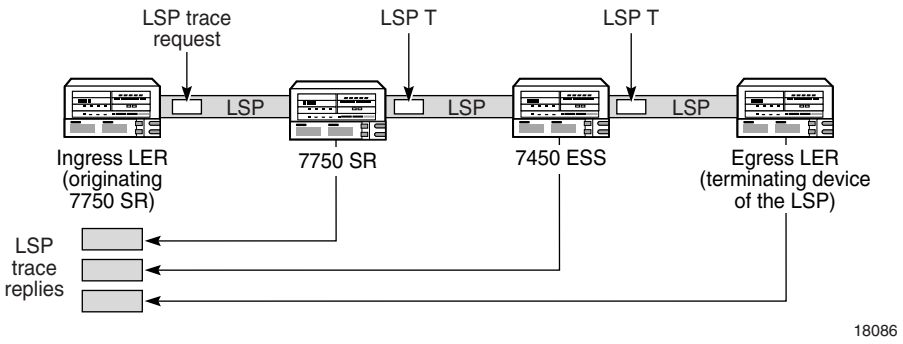
The LSP Trace OAM diagnostic tool, which is called lsp-trace in CLI, displays the hop-by-hop route used by the LSP or MPLS-TP LSP . The following information can be determined from the test:

- hop-by-hop path for an LSP or MPLS-TP LSP
- destination path of the packets

In an LSP or MPLS-TP LSP trace, the originating router creates an MPLS echo request packet for the LSP to be tested. The packet contains increasing TTL values. The MPLS echo request packet is sent and awaits a TTL exceeded response or the MPLS echo reply packet from the router that terminates the LSP. The devices along the hop-by-hop route reply to the MPLS echo request packets with TTL and MPLS echo reply information.

Figure 32-4 shows an LSP trace.

Figure 32-4 LSP Trace diagnostic



Note — The OAM messages which operate over an LDP LSP, and/or over a PW signalled by T-LDP, and which require a response using the IP path, must use a source IP address which is reachable within the same routing domain as that of the LSR ID of the LDP or T-LDP session. The messages of the LSP Trace use the T-LDP local LSR ID as the source IP address. Previously the NE's system interface address was used for this purpose.

P2MP LSP Ping OAM

The PSMP LSP Ping OAM diagnostic tool, which is called p2mp-lsp-ping in CLI, performs in-band LSP connectivity tests.

The echo request message is sent on the active P2MP instance and is replicated in the data path over all branches of the P2MP LSP instance. By default, all egress LER devices which are leaves of the P2MP LSP instance will reply to the echo request message.

You can reduce the scope of the echo reply messages by explicitly entering a list of addresses for the egress LER devices that are required to reply. A maximum of 5 addresses can be specified in a single run of the p2mp-lsp-ping command. If all 5 egress LER devices are 7x50 NEs, they will be able to parse the list of Egress LER addresses and will reply. The p2mp-lsp-ping command specifies that only the top address in the P2MP Egress Identifier TLV must be inspected by an egress LER. When interoperating with other implementations, an 7x50 egress LER will respond if its address is anywhere in the list. Furthermore, if another vendor implementation is the egress LER, only the egress LER matching the top address in the TLV may respond.

If you enter the same Egress LER address more than once in a single p2mp-lsp-ping command, the head-end NE displays a response to a single one and displays a single error warning message for the duplicate ones. When queried over SNMP, the head-end NE issues a single response trap and issues no trap for the duplicates.

P2MP LSP Trace OAM

The PSMP LSP Trace OAM diagnostic tool, which is called p2mp-lsp-trace in CLI, performs in-band LSP connectivity tests.

The LSP trace capability allows you to trace the path of a single S2L path of a P2MP LSP. Its operation is similar to that of the p2mp-lsp-ping command, but the sender of the echo reply request message includes the Downstream Detailed Mapping TLV to request the downstream branch information from a branch LSR or BUD LSR. The branch LSR or BUD LSR will then also include the Downstream Mapping TLV to report the information about the downstream branches of the P2MP LSP. An egress LER must not include this TLV in the echo response message.

The parameter probe-count operates in the same way as in the LSP Trace on a P2P LSP. It represents the maximum number of probes sent per TTL value before giving up on receiving the echo reply message. If a response is received from the traced NE before reaching maximum number of probes, then no more probes are sent for the same TTL. The sender of the echo request then increments the TTL and uses the information it received in the Downstream Detailed Mapping TLV to start sending probes to the NE downstream of the last NE which replied. This continues until the egress LER for the traced S2L path replied.

LDP Tree Trace OAM

The LDP Tree Trace OAM diagnostic tool, which is called ldp-treetrace in OAM level of the CLI, is used to detect and discover the ECMP routing paths for a LSP between egress and ingress routers. The following information is determined from the test:

- number of ECMP paths
- number of failed hops

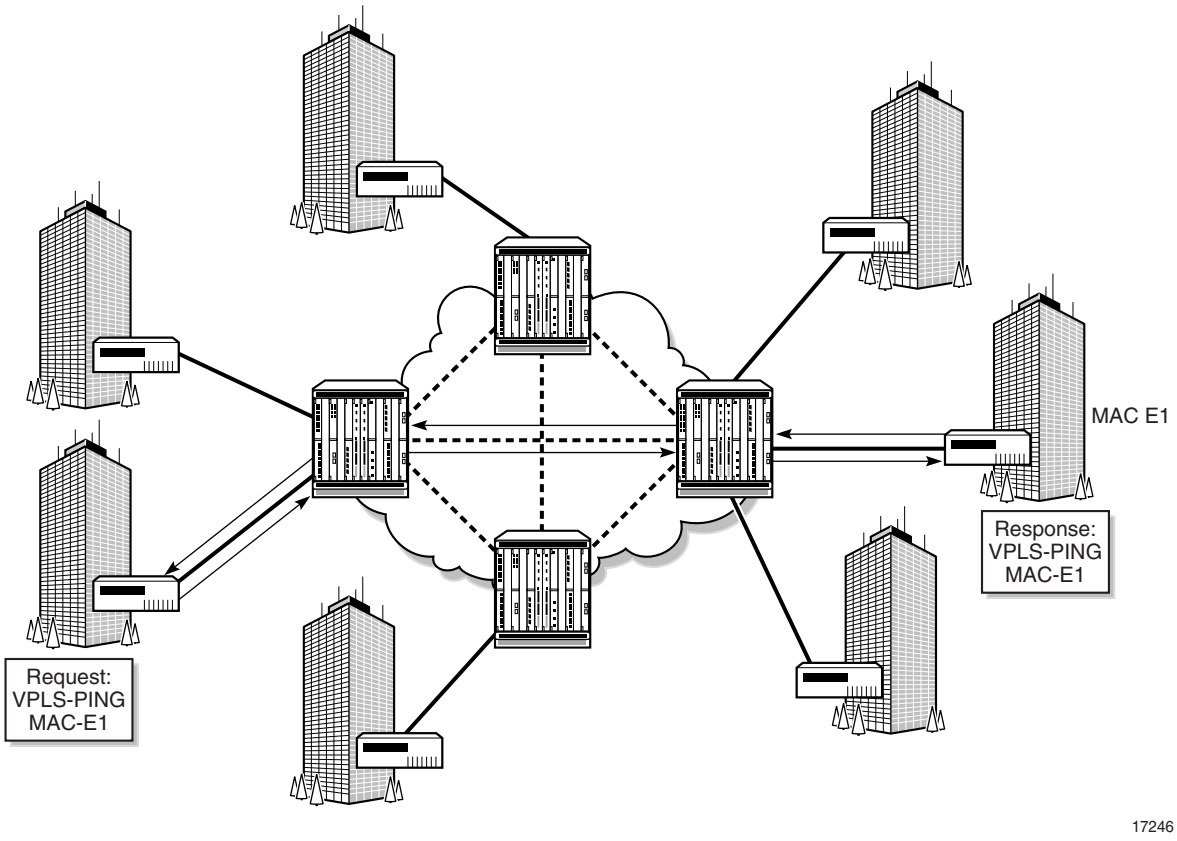
In an LDP tree trace, the originating router creates an MPLS echo request packet. The packet contains a set of IP header destination addresses. Routers along the path reply to the request with information about themselves and neighboring routers in the downstream path. The originating router uses this information to probe the downstream routers until it discovers a bit map setting common to all routers along the path. The result is a tree of available routers that the originating router can use for next hops. After discovery, the paths are tested using LSP ping and LSP trace.

Note — The OAM messages which operate over an LDP LSP, and/or over a PW signalled by T-LDP, and which require a response using the IP path, must use a source IP address which is reachable within the same routing domain as that of the LSR ID of the LDP or T-LDP session. The messages of the LDP Tree Trace use the T-LDP local LSR ID as the source IP address. Previously the NE's system interface address was used for this purpose.

MAC ping OAM

The MAC ping OAM tool, which is called mac-ping in CLI, is used to test connectivity in a VLL or VPLS by verifying a remote MAC address at the far end of a service. Figure 32-5 shows a sample MAC ping from one end of a service to the far-end MAC address of the service.

Figure 32-5 Sample MAC ping diagnostic



The MAC ping determines the existence of the far-end egress point of the service. MAC pings can be sent in-band or out-of-band. You must specify either:

- the target (far-end) MAC address
- the broadcast address

In a MAC ping that is out-of-band, the ping is forwarded along the flooding domain when no MAC address bindings exist or is sent along the bindings if MAC address bindings exist. A response ping is sent from the far-end device when there is an egress binding for the service.

In a MAC ping that is in-band, the ping is sent with a VC label TTL of 255. The ping packet goes across each hop, and when it reaches the egress router, it is identified by the OAM label and the response is sent back along the management plane.

MAC trace OAM

The MAC trace OAM tool, which is called mac-trace in CLI, displays the hop-by-hop route of MAC addresses used to reach the target MAC address at the far end of a service. MAC traces can be sent in-band or out-of-band.

You must specify either:

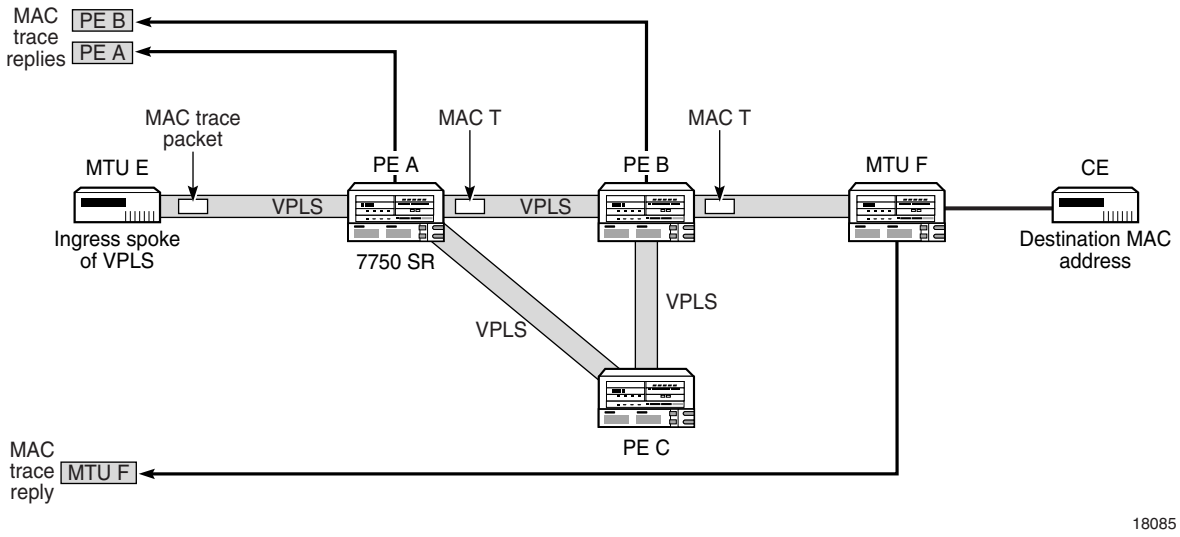
- the target (far-end) MAC address
- the broadcast address

In a MAC trace that is out-of-band, the destination IP address is specified by mapping the destination MAC address. If the destination MAC address is known to be a specific site, the far-end IP address of the service tunnel is used. If the destination MAC address is not known, the packet is sent to all service tunnels in the service.

In a MAC trace that is in-band, the trace request contains tunnel encapsulation, VC label, OAM, and other information. If the destination MAC address is known, the appropriate tunnel encapsulation and VC label is used. If the destination MAC address is not known, the packet is sent to all service tunnels, including all necessary tunnel encapsulation and egress VC labels for each bound service tunnel.

Figure 32-6 shows a MAC trace.

Figure 32-6 MAC trace diagnostic



MAC populate OAM

The MAC populate OAM tool, which is called mac-populate in CLI, is used to:

- Know whether the FIB table is accurate by testing forwarding plan correctness. This is done by populating a service FIB with an OAM-tagged MAC entry. This MAC entry indicates that the NE is the egress NE for the MAC address of a service. You can then use the FIB manager to see the OAM-tagged MAC entry.
- Send a message through the flooding domain to learn a MAC address, as if a customer packet with that source MAC address had flooded the domain from that ingress point of the service.

You can:

- force an existing MAC address to become OAM-tagged
- distinguish, in the FIB manager, MAC addresses that are OAM-tagged
- age an OAM-tagged MAC address

In a MAC populate, the OAM-tagged MAC address is populated on the egress point of the service. You can specify whether to flood this OAM-tagged MAC address to other devices so that the same OAM-tagged entry is added to the FIB tables of other devices.

MAC purge OAM

The MAC purge OAM tool, which is called mac-purge in CLI, is used to delete an OAM-tagged entry from a FIB, which was generated using the MAC populate OAM tool. This clears the FIB of any learned information for a specific MAC address, allows the FIB to be populated only by a MAC populate request, and can be used to flush all devices in a service domain.

CPE ping

The CPE ping tool, which is called cpe-ping in the CLI, is used to trace the end-to-end switching of specified MAC addresses of customer premises equipment. This ping extends the functionality of the MAC ping beyond the egress (customer-facing) port by allowing a ping to the SAP of a VPLS or a VLL Epipe service over a VPLS PBB backbone.

ANCP loopback

The ANCP loopback test, which is called oam ancp in the CLI, is used to send DSL OAM commands to complete an OAM test from a centralized point or when operational boundaries prevent direct access to the DSLAM. The ANCP loopback test raises an alarm that generates a log event displaying both successful and failed results.

F5 OAM loopback

The F5 OAM loopback test is used to validate ATM bonding on DSL ports. The parameters for the F5 OAM loopback test are only visible when a DSL module is connected to an ISAM device with the bonding type of ATM and the device is operationally up.

VPRN ping and VPRN trace

The VPRN ping and VPRN trace OAM tools are enabled from the VRF site of the subscriber's VPRN service. The VPRN ping determines the existence of the far-end egress point of the service. This allows testing of whether a specific destination can be reached. VPRN pings can be sent in-band or out-of-band.

The VPRN trace displays the hop-by-hop path for a destination IP address within a VPRN service. This allows operators to know the destination path of customer traffic. VPRN traces can be sent in-band or out-of-band.

For both the VPRN ping and VPRN trace tests, when a test packet is sent, a reply is generated if the targeted prefix is reachable over a VPRN SAP or VPRN spoke interface. Otherwise the test packet is dropped in CPM. This also applies in the case of a routed VPLS interface.

ATM OAM ping

The ATM OAM ping tool, which is called atmoam-ping in CLI, performs an ATM ping on an existing ATM PVC from the PVC endpoint using ATM OAM loopback cells. An ATM ping tests VC integrity and endpoint connectivity for PVCs using OAM loopback capabilities.

Multicast FIB ping

The multicast FIB ping OAM tool, which is called mfib-ping in CLI, identifies the SAPs that egress an IP multicast stream within a VPLS. This diagnostic can also be used to display the SAPs that are operationally up in the VPLS.

Multicast router information

The multicast router information OAM tool, which is called mrinfo in CLI, identifies VPRN multicast information for the target router. The information includes details that are related to adjacent routers, supported protocols, traffic metrics, and time-to-live thresholds. Administrators can use this information to identify bidirectional adjacency relationships.

Multicast trace

The multicast trace OAM tool, which is called mtrace in CLI, identifies the hop-by-hop route used by VPRN multicast traffic to reach the target router. This diagnostic gathers the hop address, routing error conditions, and packet statistics at each hop. The 5620 SAM attempts to trace the receiver-to-sender route for the traffic. The destination of the diagnostic can be any PIM-enabled interface in the routing instance.

In this test, the command sends a ping to the head of the specified multicast group (which can be one or more hops away from the launch NE). If that ping fails, the command will ping the neighboring NE, then the neighbor's neighbor, and so on up the multicast group chain to determine which NE fails to respond.

ICMP ping

The ICMP ping OAM tool, which is called icmp-ping in CLI, identifies the reachability of a remote host across the IP network. The tool is used with ICMP trace to detect and localize faults in IP networks.

The ICMP ping OAM tool can also be enabled from the VRF site of the subscriber's VPRN service. An ICMP ping determines the existence of the far-end egress point of the service. This allows testing of whether a specific destination can be reached. ICMP pings can be sent in-band or out-of-band.

ICMP trace

The ICMP trace OAM tool, which is called icmp-trace in CLI, identifies the diagnostic used to trace the ICMP traceroute control table. The tool is used with ICMP ping to detect and localize faults in IP networks.

ICMP trace displays the hop-by-hop path for a destination IP address within a VPRN service. This allows operators to know the destination path of subscriber traffic. ICMP traces can be sent in-band or out-of-band.

OmniSwitch ping and traceroute

The 5620 SAM supports OmniSwitch ping and traceroute by using user-defined CLI scripts. See Procedure 32-38 for information about creating an OmniSwitch OAM script. See Procedures 32-40 and 32-41 for information about configuring and running OmniSwitch OAM scripts.

DNS ping

The DNS ping OAM tool, which is called dns-ping in CLI, identifies the diagnostic used to ping the DNS name, if DNS name resolution is configured.

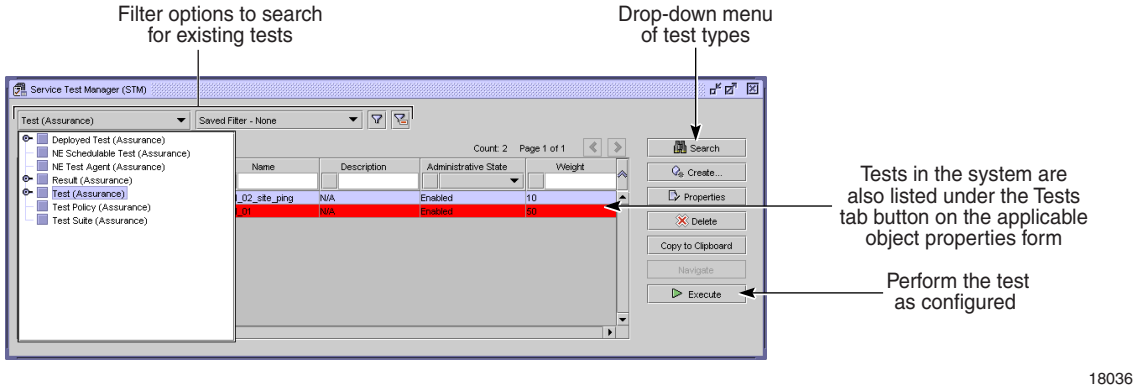
Service assurance test management and configuration

There are two main types of forms for the service assurance test manager.

- Browse and list manager, to generate lists of OAM diagnostics and to run OAM diagnostics
- Configuration form, to create or modify service assurance tests and review the results of service assurance tests

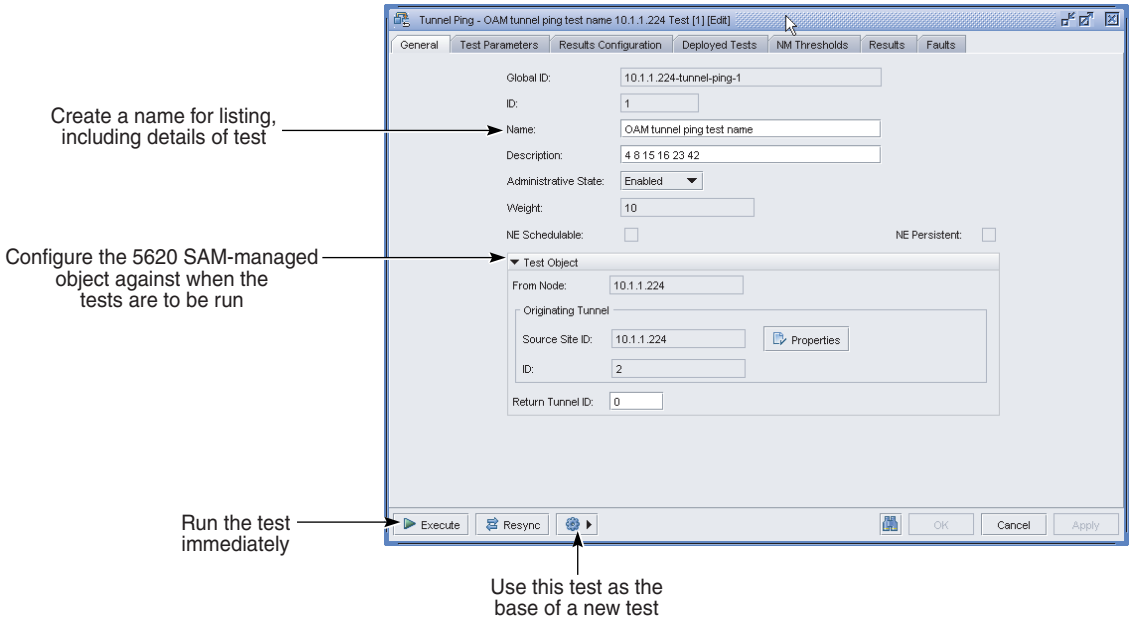
Figure 32-7 shows the browse and list manager form.

Figure 32-7 Service assurance test manager browse and list form



Each service assurance test configuration form contains multiple tabs. Figure 32-8 shows a sample service assurance OAM test with the General tab displayed.

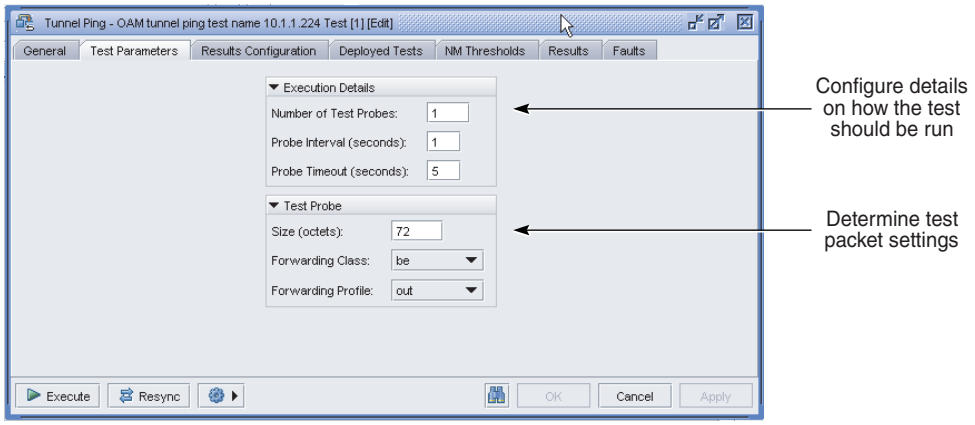
Figure 32-8 Service assurance OAM test configuration form - General



18037

Figure 32-9 shows the same sample service assurance OAM test with the Test Parameters tab displayed.

Figure 32-9 Service assurance OAM test configuration form - Test Parameters tab



18034

Figure 32-10 shows the same sample service assurance OAM test with the Results Configuration tab displayed.

Figure 32-10 Service assurance OAM test configuration form - Results Configuration

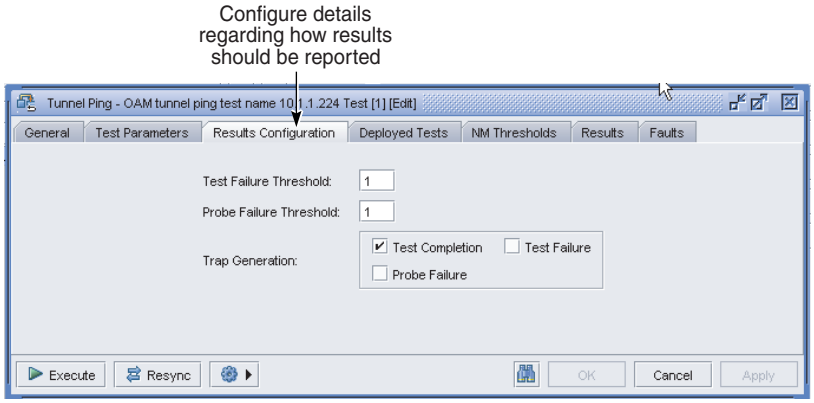


Figure 32-11 shows the same sample service assurance OAM test with the Results tab displayed. Selecting the Results tab opens an additional form, which provides detailed test results, including OAM test packet details, when the OAM test involves sending test packets.

Figure 32-11 Service assurance OAM test configuration form - Results

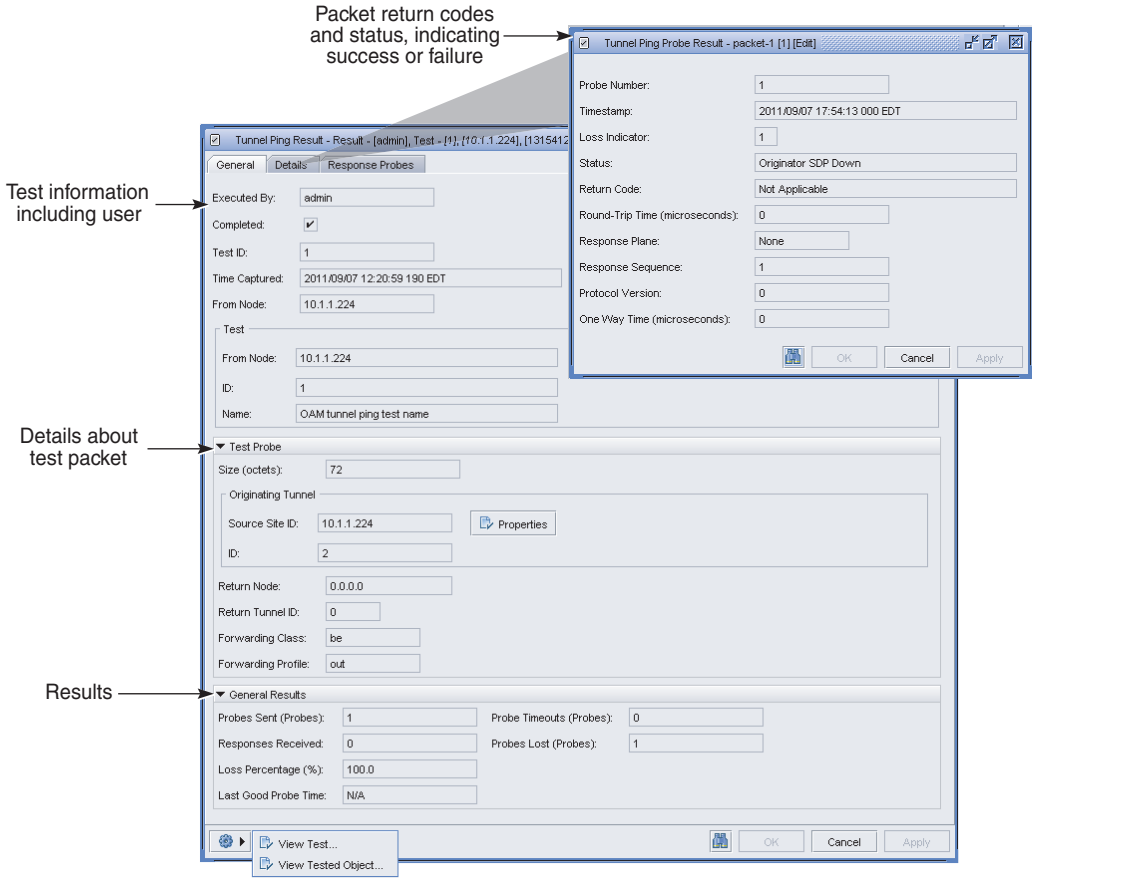
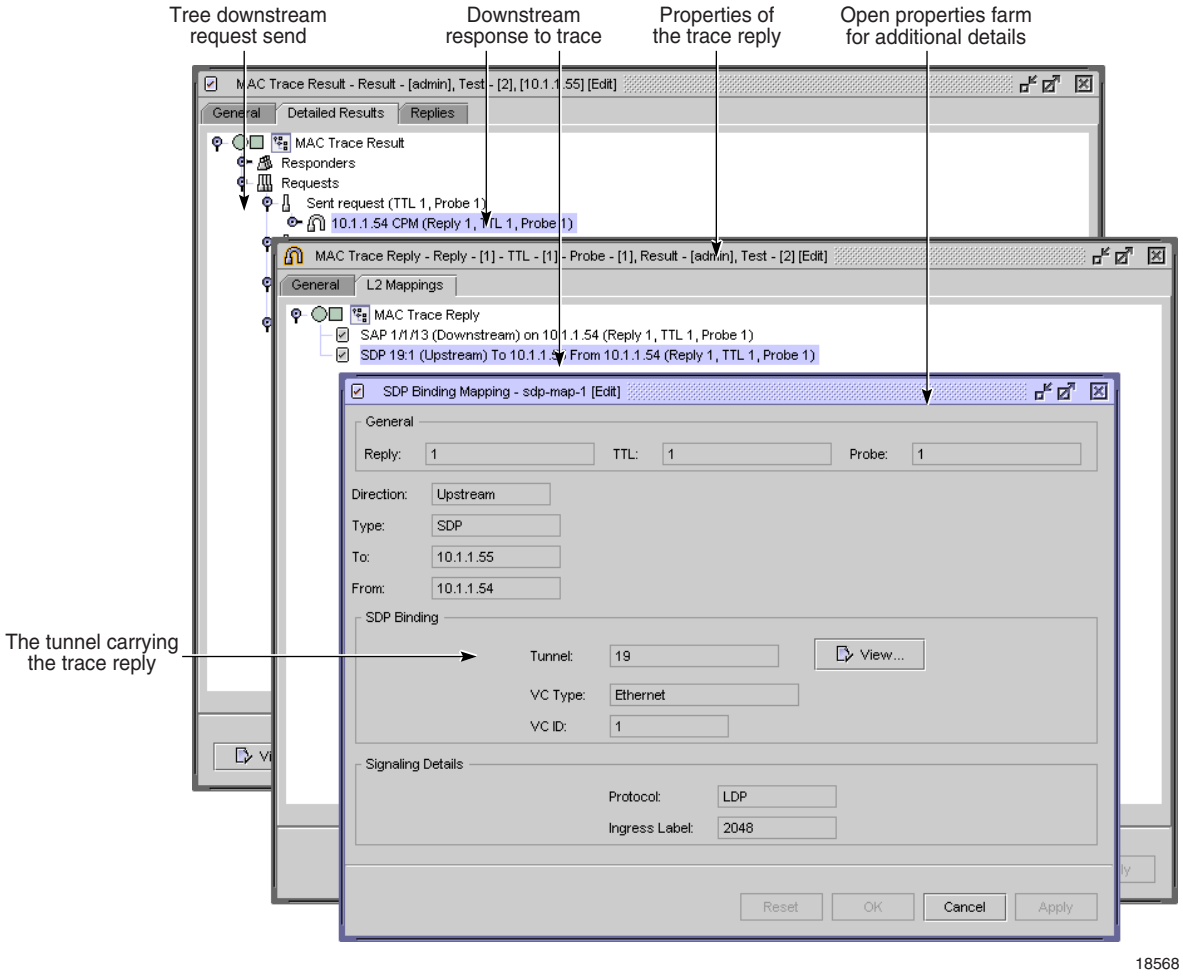


Figure 32-12 shows the information from a sample MAC trace. Trace probe information is available from the Detailed Results tab. Continue to navigate down from the trace requests to view result information.

Figure 32-12 Service assurance OAM test probe and trace results details



32.2 Sample OAM diagnostic test configuration

Figure 32-13 shows a sample OAM diagnostic sequence, illustrating how you can use multiple OAM tests to verify service creation and diagnose service problems. This sample shows a VPLS.

Figure 32-13 Sample OAM diagnostic sequence for a VPLS

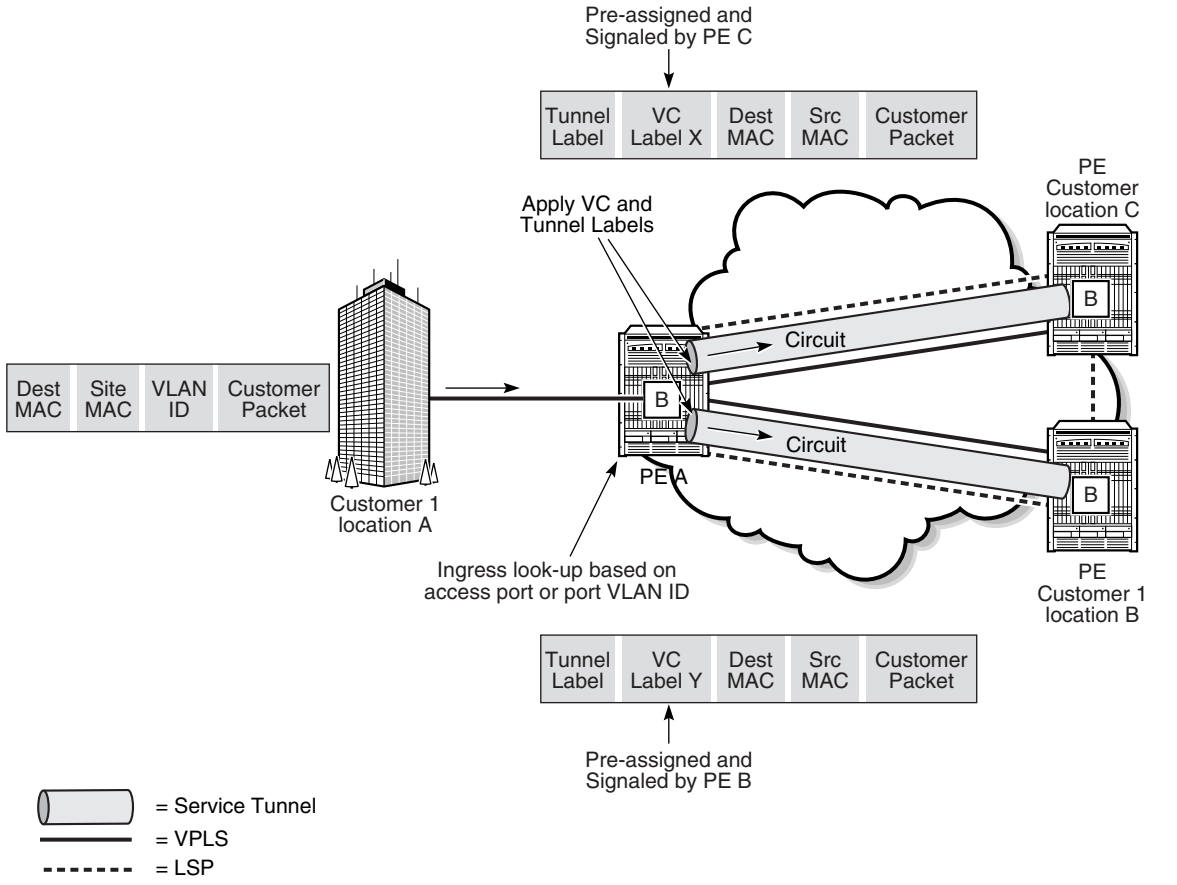


Table 32-2 lists the high-level tasks necessary to configure this sample.

Table 32-2 Sample OAM diagnostic configuration for a service

Task	Description
Service creation and OAM validation	
1. MPLS and LSP creation	Create an MPLS network and LSPs for use by the service tunnels connecting the VPLS sites. Test the validity of the LSPs using LDP tree trace or LSP ping. If the results indicate a problem with the path, use LSP trace to check the specific MPLS path for the device causing the ping failure.
2. Service tunnel creation	Create a service tunnel that uses the MPLS LSP created earlier and perform a tunnel ping on the service tunnel to verify tunnel connectivity. Create all tunnels necessary to interconnect the VPLS sites, and repeat the tunnel ping to ensure tunnel connectivity. After all of the tunnels are created, use the tunnel ping remote tunnel option and specify the return tunnel path. Verify bidirectional tunnel connectivity.

(1 of 2)

Task	Description
3. Service creation	Create a service using the service tunnels to interconnect the VPLS sites, either using mesh or spoke service tunnel bindings. Use a service site ping between each VPLS site device and its neighboring sites to verify service configuration consistency.
4. MAC diagnostics	Connect the CPE devices to the VPLS and verify traffic. Use MAC trace from the edge devices to verify MAC address learning by the VPLS sites and to ensure that the correct associations are made between MAC addresses and the service tunnels or SAPs to which they are bound. Use MAC ping against an unknown MAC address to verify that no response is returned. Use MAC populate to create an OAM-specific MAC address. Use MAC ping and MAC trace against the created MAC address to verify that customer traffic is not affected by the additional MAC address. Use MAC purge to remove the created OAM MAC address.
Service OAM diagnostics	
1. Diagnose traffic flow problems at a specific MAC address	Use MAC ping against the MAC address to which traffic is not flowing. Use the source and destination MAC address to simulate customer traffic routes as closely as possible. Use MAC trace to pinpoint the location of the traffic failure. Check for MAC filter rules or MAC table sizes to identify possible causes of the failure, for example, incorrect configurations.
2. Diagnose the components of the service	Use service site ping to test the potential next hops to ensure consistent configuration. Use tunnel ping to the far end of the tunnel using the remote tunnel option and specify the return tunnel path. Verify bidirectional tunnel connectivity. Use LSP ping to determine if the tunnel is working. Use an LSP trace to determine if an intervening device is down.

(2 of 2)

32.3 Workflow to use OAM diagnostic tests

1. Create the transport network and customer services.
2. Monitor customer services or troubleshoot the transport network before you commission, according to your company's policies.
3. When the creation of a tunnel needs to be tested, or a customer service is compromised, use the service assurance tools to troubleshoot the problem.



Note 1 — All of the tests mentioned in this workflow are used on an as-required basis.

Note 2 — Not all service assurance tools are applicable to every NE managed by the 5620 SAM.

i. Use MTU ping to troubleshoot and resolve tunnel and service problems that are related to frame size across all equipment that is used by the service or tunnel. See Procedures 32-1 and 32-2 for more information.

ii. Use tunnel ping to troubleshoot and resolve tunnel and service problems that are related to issues that circuits may have transmitting traffic across the GRE or MPLS network. See Procedures 32-3 and 32-4 for more information.

iii Perform Ethernet CFM tests to provide path discovery and fault detection, isolation, and notification in an L2 network. As required, perform any of the following tests:

- CFM Global MEG OAM; see Procedure 32-5.
- CFM CC OAM; see Procedure 32-6.
- CFM loopback; see Procedure 32-7.
- CFM link trace; see Procedure 32-8.
- CFM Eth test; see Procedure 32-9.
- CFM one-way delay; see Procedure 32-10.
- CFM two-way delay; see Procedure 32-11.
- CFM single-ended loss; see Procedure 32-12.
- CFM two-way SLM; see Procedure 32-13.

iv Use service site ping to troubleshoot and resolve service problems that are related to the end-to-end connectivity of a customer service within the provider network. See Procedure 32-21 for more information.

v Use VCCV ping and VCCV trace to troubleshoot and resolve issues that are related to VPLS/MVPLS/HVPLS and VLL services. (Note that the VCCV trace test definition only applies to VLL services.) See Procedures 32-23 and 32-24 for more information.

vi Use LDP tree trace to detect and discover available routers for ECMP routing. See Procedure 32-29 for more information.

vii Use LSP ping and LSP trace to troubleshoot and resolve problems that are related to MPLS LSPs, MPLS-TP LSPs, LDPs, and MPLS paths. See Procedures 32-25 and 32-26 for more information.

viii Use P2MP LSP Ping and P2MP LSP Trace to perform in-band LSP connectivity tests. See Procedures 32-27 and 32-28 for more information.

ix Use MAC ping (Procedure 32-17), MAC trace (Procedure 32-18), MAC populate (Procedure 32-15), MAC purge (Procedure 32-16), and CPE ping (Procedure 32-19) to troubleshoot and resolve problems that are related to FIBs and MAC addressing. The tests are used in combination; for example, MAC populate to inject a MAC address into the network, MAC ping to determine where the address was learned, MAC trace to determine the path, CPE ping to test the VPLS, and MAC purge to remove the injected MAC address.

x Use ANCP loopback to send OAM messages to the access NE. See Procedure 32-20 for more information.

xi Use F5 OAM loopback to validate ATM bonding on DSL ports. See Procedure 32-22 for more information.

xii Use VPRN ping, VPRN trace, ICMP ping and ICMP trace to troubleshoot and resolve problems with a VPRN service. See Procedures 32-14, 32-35, and 32-36 for more information.

xiii Use ATM ping and ATM loopback to test ATM PVC connections. See Procedures 32-33 and 32-34 for more information.

xiv Use multicast FIB ping to troubleshoot and resolve problems with the multicast component of a VPLS. See Procedure 32-32 for more information.

xv Use multicast router information and multicast trace to troubleshoot and resolve problems with the multicast component of a VPRN service. See Procedures 32-30 and 32-31 for more information.

xvi Use ICMP ping (Procedure 32-35), ICMP trace (Procedure 32-36), and DNS ping (Procedure 32-37) to troubleshoot and resolve problems with IP reachability.

xvii Use Procedure 32-42 to configure an 802.3ah EFM diagnostic at the NE or port level.

xviii (OmniSwitch only) Use OmniSwitch ping and traceroute scripts to troubleshoot and resolve problems with IP reachability on an OmniSwitch. See Procedures 32-38, 32-40, and 32-41 for more information.

xix (OmniSwitch only) Use OmniSwitch advanced loopback to troubleshoot and resolve problems on an OmniSwitch port. See Procedure 32-39 for more information.

xx (OmniSwitch only) Use Procedure 32-43 to configure an 802.3ah EFM diagnostic on an OmniSwitch at the NE or port level.

4 Use Procedures 32-46 and 32-47 to configure NM threshold-crossing alarms for OAM tests that are NE-schedulable and non-NE-schedulable, respectively.

5 Use Procedure 32-50 to set STM managed device test limits.

6 Use the OAM tool diagnostic response messages and results form information to resolve the customer service problem. See Procedures 32-44 and 32-45 for more information.

7 Use Procedures 32-48 and 32-49 to edit or delete an OAM diagnostic test, respectively.

32.4 OSS OAM Test Results file retrieval

OSSI clients can use the <registerSasLogToFile> method to receive OAM logs that are based on specific class types. Clients must register to receive the logs, and if no client registers, no logs are created. Refer to the *5620 SAM XML OSS Interface Developer Guide* for detailed information on OSSI client operations.

OAM data is exported to the file after the data is read from the NE. The file is saved to a specified directory on the 5620 SAM server.

Prior to enabling OSSI clients to receive Test Results files, you should configure the DB Test Result Retention Time (hours), Default Test Result Storage, and Log Retention Time (minutes) parameters as required. These are accessed by clicking Administration→System Preferences and then clicking the Test Manager tab.

32.5 OAM diagnostic tests procedures

Use the following procedures to create and execute OAM diagnostic tests.

Procedure 32-1 To create and run an MTU ping OAM diagnostic from a service tunnel

Use the MTU ping diagnostic to find the largest valid frame size.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form opens.

2 Filter to list only the source and destination routers of the service tunnel and click on the Search button. The list of service tunnels appears.

3 Double-click on a service tunnel from the list. The Tunnel (Edit) form opens.

4 Click on the Tests tab.

5 Click on the MTU Ping tab.

6 Click on the Create button. The MTU Ping (Create) form opens with the General tab displayed. The form displays information about the service tunnel being tested and the originating tunnel ID.

7 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State

8 Click on the Test Parameters tab and configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Size (octets)
- MTU Start Size (octets)
- MTU End Size (octets)
- MTU Step Size (octets)



Note — If the step size is small but the end message size is large, the amount of time to complete the MTU ping may be many minutes. Ensure that you have an appropriate step size that reflects the range of MTU packet sizes you want to test.

9 Click on the Results Configuration tab and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Packet Failure Threshold
- Trap Generation

10 Click on the Apply button to save the changes.

11 Perform the MTU ping.

i Click on the Execute button in the MTU Ping (Edit) form. The MTU ping diagnostic starts. A deployed test is created and run. Open the deployed test from the Deployed Tests tab to view its current state. When the test is complete, the deployed test is removed, and you can view the results. The diagnostic is complete.

ii Click on the Results tab. The list of MTU ping OAM probes sent is displayed.

iii Click on the row(s) as appropriate to view diagnostic information.

iv Click on the Properties button. The OAM results form opens. The diagnostic information includes:

- source and destination of the diagnostic
- timestamp of when the test was completed
- time to complete the diagnostic, in milliseconds
- frame size sent
- OAM diagnostic status
- diagnostic code returned

See Procedure 32-45 for more information about the diagnostic status messages. Use the status message to interpret the diagnostic results. For example, the status message Response Received indicates that the MTU OAM diagnostic completed successfully.

v Close the form.

12 Close the Tunnel (Edit) form when the OAM diagnostics are complete.

Procedure 32-2 To create an MTU ping OAM diagnostic from the test manager

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Service Transport→Create MTU Ping from the Create contextual menu. The MTU Ping (Create) form opens.

4 Configure the parameters described in Procedure 32-1. You must additionally configure the source of the service tunnel.

i Click on the Select button beside the Source Site ID parameter. The Select Originating Tunnel form opens.

ii Click on the Search button.

iii Select a tunnel from the list.

iv Click on the OK button. The MTU Ping (Create) form reappears with the IP address and ID of the selected service tunnel.

5 Click on the Apply button to save the changes.

6 Open the deployed test from the Deployed Tests tab to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

7 Click on the Execute button to start the ping. A deployed test is created and run.

8 View the test results on the Results tab. The results depend on the type of test. See Procedure 32-44. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 32-3 To create and run a tunnel ping OAM diagnostic from a service tunnel

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form opens.

2 Filter to list only the source and destination routers of the service tunnel and click on the Search button. The list of service tunnels opens.

3 Double-click on a service tunnel from the list. The Tunnel (Edit) form opens.

4 Click on the Tests tab.

5 Click on the Tunnel Ping tab.

6 Click on the Create button. The Tunnel Ping (Create) form opens with the General tab displayed. The form displays information about the circuit being tested, including the originating tunnel ID.

7 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- Return Tunnel

8 Click on the Test Parameters tab and configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Probe History
- Size (octets)
- Forwarding Class
- Forwarding Profile

The Packet Interval (seconds) parameter has an effect only when multiple probes are to be sent.

The Probe History parameter is only configurable when the NE Schedulable parameter is enabled.

Ensure that you configure the Forwarding Class parameter to work with the services that use the tunnel.

9 Click on the Results Configuration tab and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Packet Failure Threshold
- Trap Generation

10 Click on the Apply button to save the changes.

11 Confirm the action. The created tunnel ping test appears in the list of tests on the Tunnel Ping tab of the Tunnel (Edit) form.

12 Perform the tunnel ping OAM diagnostic:

i Click on the Execute button in the Tunnel Ping (Edit) form. A deployed test is created and run. Open the deployed test from the Deployed Tests tab to view its current state. When the test is complete, the deployed test is removed, and you can view the results. The diagnostic is complete.

ii Click on the Results tab. The list of tunnel ping OAM packets sent is displayed.

iii Click on the row(s) as appropriate to view diagnostic information.

iv Click on the Properties button. The OAM results form opens. The diagnostic information includes:

- source and destination of the diagnostic
- timestamp of when the test was completed
- time to complete the diagnostic, in milliseconds
- OAM diagnostic status
- diagnostic code returned

See Procedure 32-45 for more information about the diagnostic status messages. Use the status message to interpret the diagnostic results.

v Close the form.

13 Close the Tunnel (Edit) form when the OAM diagnostics are complete.

Procedure 32-4 To create a tunnel ping OAM diagnostic from the test manager

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Service Transport→Create SDP Ping from the Create contextual menu. The Tunnel Ping (Create) form opens.

4 Configure the parameters described in Procedure 32-3. You must additionally configure the source of the service tunnel.

   i Click on the Select button beside the Source Site ID parameter. The Select Originating Tunnel form opens.

   ii Configure the filter criteria.

   iii Click on the Search button.

   iv Select a tunnel from the list.

   v Click on the OK button. The Tunnel Ping (Create) form reappears with the IP address and ID of the selected service tunnel.

5 Click on the Apply button to save the changes.

6 Click on the Execute button to start the tunnel ping. A deployed test is created and run.

7 Open the deployed test from the Deployed Tests tab to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

8 View the test results on the Results tab. The results depend on the type of test. See Procedure 32-44. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 32-5 To create and execute a CFM Global MEG OAM diagnostic

Perform this procedure to manually create and execute a CFM Global MEG test.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button and choose Ethernet CFM→CFM Global MEG from the menu. The Global Maintenance Entity Group, Test (Create) form opens.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- NM Administrative State

4 To configure parameters in the Maintenance Domain tab, Maintenance Entity Group and Initial MEG configuration, see Procedure 78-1 for more information.

5 Click on the Apply button. The form displays additional buttons and tabs.

6 To execute the test, click on the Test tab and select the Test to be executed. Select the test and click on the Properties button, the CFM Continuity Check (Edit) form.

7 Click on the Results tab to view the test results. See Procedure 32-44 for information about test results.

8 Close the CFM Continuity Check Test (Edit) form.

Procedure 32-6 To create and execute a CFM Continuity Check OAM diagnostic

Perform this procedure to manually create and execute a CFM Continuity Check test.



Note — The 5620 SAM automatically creates a CFM CC test when you create an MD and global MEG. You can execute an automatically created test using the STM, or from the Tests tab of a MEG.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button and choose Ethernet CFM→Create Continuity Check from the menu. The CFM Continuity Check Test (Create) form opens.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- Duration (minutes)

4 If you are configuring the test for a 7705 SAR, configure the parameters in the Initial Dual Ended Loss Test Options panel:

- Enable Test
- Alarm Threshold (%)
- Alarm Clearing Threshold (%)

5 Click on the Select button. The Select Maintenance Entity Group form opens.

6 Specify a search filter, if required, and click on the Search button. A list of MEGs is displayed.

7 Select a MEG in the list and click on the OK button. The Select Maintenance Entity Group form closes, and the MEG is displayed on the CFM Continuity Check Test (Create) form.

8 Click on the Apply button. The form displays additional buttons and tabs.

9 To execute the test, click on the Execute button on the CFM Continuity Check (Edit) form.

10 Click on the Results tab to view the test results. See Procedure 32-44 for information about test results.

11 Close the CFM Continuity Check Test (Create) form.

Procedure 32-7 To create and execute a CFM loopback diagnostic

Perform this procedure to manually create and execute a CFM loopback test. You can create multiple CFM loopback tests for an originating MEP.

You can also perform multicast loopbacks by providing a multicast address (class 1 multicast destination) which aligns with the level that the originating MEP is configured on. Only one multicast test can be run at a time per NE, and results from the previous test are deleted when a new test is started. The stored values include the responding MEP MAC address, the sequence number, and a locally-assigned rx index (allowing you to detect out-of-order responses).



Note — The maximum number of continuous CFM loopback tests that can be executed is 300, provided that the SAA packet per second rate of 200 pps is not exceeded. The total number of continuous tests must share this maximum rate of 200 pps.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Ethernet CFM→CFM Loopback from the contextual menu. The CFM Loopback Test (Create) form opens.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- NM Administrative State
- NE Schedulable



Note — If the NE Schedulable parameter is enabled, an additional tab titled Results Configuration is displayed for the form.

5 Click on the Select button beside the Global ID field to choose a global MEG. The Select Global MEG - CFM Loopback form opens.

6 Specify a search filter, if required, and click on the Search button. A list of global MEGs is displayed.

7 Select an entry and click on the OK button. The Select Global MEG - CFM Loopback form closes, and the CFM Loopback (Create) form displays the global MEG.

8 Click on the Select button beside the ID field to choose an originating MEP. The Select Originating MEP - CFM Loopback form opens.

9 Specify a search filter, if required, and click on the Search button. A list of MEPs is displayed.

10 Select a MEP in the list and click on the OK button. The Select Originating MEP - CFM Loopback form closes, and the CFM Loopback (Create) form displays the MEP information.

11 Perform one of the following:

a To select the test destination using the target's MAC Address, go to step 14.

b To select the test destination using the target's MEP ID, continue to step 12.



Note — MEP ID selection is only supported for OmniSwitch NEs. The NE Schedulable parameter must be enabled in step 4.

12 Enable the Enable Target MEP ID parameter.

13 Perform one of the following:

a Configure the Target MEP ID parameter.

b Select a MEP as the test destination. Perform the following steps.

i Click on the Select MEP button beside the Target MEP ID parameter to choose the destination MEP. The Select MEP - CFM Loopback form opens.

ii Select an entry and click on the OK button. The Select MEP - CFM Loopback form closes, and the CFM Loopback (Create) form refreshes.

14 Perform one of the following:

a Select a MEP as the test destination. Perform the following steps.

i Click on the Select MEP button beside the Target MAC Address parameter to choose the destination MEP. The Select MEP - CFM Loopback form opens.

ii Select an entry and click on the OK button. The Select MEP - CFM Loopback form closes, and the CFM Loopback (Create) form refreshes.

b Select a MIP as the test destination. Perform the following steps.

i Click on the Select MIP button beside the Target MAC Address parameter to choose the destination MIP. The Select MIP - CFM Loopback form opens.

ii Select an entry and click on the OK button. The Select MIP - CFM Loopback form closes, and the CFM Loopback (Create) form refreshes.



Note — MIP selection is not supported for OmniSwitch NEs.

c Select an unmanaged MEP as the test destination. Perform the following steps.

i Click on the Select Unmanaged MEP button beside the Target MAC Address parameter to select the destination MEP. The Select Unmanaged MEP - CFM Loopback form opens.

ii Select an entry and click on the OK button. The Select Unmanaged MEP - CFM Link Trace form closes, and the CFM Loopback (Create) form refreshes.

15 If the NE Schedulable parameter was enabled in step 4 then go to step 17. Otherwise, go to step 16.

16 Configure the MEP Transmit LBM Information parameters:

- Data Size
- VLAN Priority
- Number of Loopback Sent
- VLAN Drop Enable

17 Click on the Test Parameters tab and configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Forwarding Class
- Forwarding Profile
- Size (octets)
- Test Interval (minutes)
- Probe History
- Continuous Execution

The Probe History parameter is only configurable when the NE Schedulable parameter is enabled.

18 Click on the Results Configuration tab and configure the parameters:

- Test Failure Threshold
- Packet Failure Threshold
- Trap Generation
- Accounting Files
- Test Result Storage

The Trap Generation parameter is only configurable when the Accounting Files parameter is disabled.

The Test Result Storage parameter is only configurable when the Accounting Files parameter is enabled.

19 Click on the Apply button to save the changes.

20 To execute the test, click on the Execute button.

21 Click on the Results tab to view the test results. See Procedure 32-44 for information about test results.

Procedure 32-8 To create and execute a CFM link trace diagnostic



Note — The maximum number of continuous CFM link trace tests that can be executed is 300, provided that the SAA packet per second rate of 200 pps is not exceeded. The total number of continuous tests must share this maximum rate of 200 pps.

However, it is recommended that number of continuous CFM link trace tests executed should be kept well below the maximum allowed limit.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Ethernet CFM→CFM Link Trace from the Create contextual menu. The CFM Link Trace (Create) form opens.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- NM Administrative State
- NE Schedulable



Note — If the NE Schedulable parameter is enabled, two additional tabs are displayed for the form, Test Parameters and Results Configuration.

5 Click on the Select button beside the Global ID field to choose a global MEG. The Select Global MEG - CFM Link Trace form opens.

6 Specify a search filter, if required, and click on the Search button. A list of global MEGs is displayed.

7 Select an entry and click on the OK button. The Select Global MEG - CFM Link Trace form closes, and the CFM Link Trace (Create) form displays the global MEG.

8 Click on the Select button beside the ID field to choose an originating MEP. The Select Originating MEP - CFM Link Trace form opens.

9 Specify a search filter, if required, and click on the Search button. A list of MEPs is displayed.

10 Select a MEP in the list and click on the OK button. The Select Originating MEP - CFM Link Trace form closes, and the CFM Link Trace (Create) form displays the MEP information.

11 Perform one of the following:

a Select a MEP as the test destination. Perform the following steps.

i Click on the Select MEP button beside the Target MAC Address parameter to select the destination MEP. The Select MEP - CFM Link Trace form opens.

ii Select an entry and click on the OK button. The Select MEP - CFM Link Trace form closes, and the CFM Link Trace (Create) form refreshes.

b Select a MIP as the test destination. Perform the following steps.

i Click on the Select MIP button beside the Target MAC Address parameter to select the destination MIP. The Select MIP - CFM Link Trace form opens.

ii Select an entry and click on the OK button. The Select MIP - CFM Link Trace form closes, and the CFM Link Trace (Create) form refreshes.

c Select an unmanaged MEP as the test destination. Perform the following steps.

i Click on the Select Unmanaged MEP button beside the Target MAC Address parameter to select the destination MEP. The Select Unmanaged MEP - CFM Link Trace form opens.

ii Select an entry and click on the OK button. The Select Unmanaged MEP - CFM Link Trace form closes, and the CFM Link Trace (Create) form refreshes.

12 If the NE Schedulable parameter was enabled in step 4 then go to step 15. Otherwise, continue to step 13.

13 Configure the MEP Transmit LTM Information TTL parameter.

14 Go to step 17.

15 Click on the Test Parameters tab and configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Forwarding Class
- Forwarding Profile
- Probe History
- TTL
- Continuous Execution

The Probe History parameter is only configurable when the NE Schedulable parameter is enabled.

16 Click on the Results Configuration tab and configure the parameters:

- Maximum Failures
- Trap Generation
- Accounting Files
- Test Result Storage

The Trap Generation parameter is only configurable when the Accounting Files parameter is disabled.

The Test Result Storage parameter is only configurable when the Accounting Files parameter is enabled.

17 Click on the Apply button to save the changes.

18 To execute the test, click on the Execute button.

19 Click on the Results tab to view the test results. See Procedure 32-44 for information about test results.

Procedure 32-9 To create and execute a CFM Eth test diagnostic

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Ethernet CFM→CFM Eth Test from the Create contextual menu. The CFM Eth Test (Create) form opens.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- NM Administrative State

5 Click on the Select button beside the Global ID field to choose a global MEG. The Select Global MEG - CFM Eth Test form opens.

6 Specify a search filter, if required, and click on the Search button. A list of global MEGs is displayed.

7 Select an entry and click on the OK button. The Select Global MEG - CFM Eth Test form closes, and the CFM Eth Test (Create) form displays the global MEG.

8 Click on the Select button beside the ID field to choose an originating MEP. The Select Originating MEP - CFM Eth Test form opens.

9 Specify a search filter, if required, and click on the Search button. A list of MEPs is displayed.

10 Select a MEP in the list and click on the OK button. The Select Originating MEP - CFM Eth Test form closes, and the CFM Eth Test (Create) form displays the MEP information.

11 Perform one of the following.

a Select a MEP as the test destination. Perform the following steps.

i Click on the Select MEP button beside the Target MAC Address parameter to select the destination MEP. The Select MEP - CFM Eth Test form opens.

ii Select an entry and click on the OK button. The Select MEP - CFM Eth Test form closes, and the CFM Eth Test (Create) form refreshes.

b Select a MIP as the test destination. Perform the following steps.

i Click on the Select MIP button beside the Target MAC Address parameter to choose the destination MIP. The Select MIP - CFM Eth Test form opens.

ii Select an entry and click on the OK button. The Select MIP - CFM Eth Test form closes, and the CFM Eth Test (Create) form refreshes.

c Select an unmanaged MEP as the test destination. Perform the following steps.

i Click on the Select Unmanaged MEP button beside the Target MAC Address parameter to select the destination MEP. The Select Unmanaged MEP - CFM Eth Test form opens.

ii Select an entry and click on the OK button. The Select Unmanaged MEP - CFM Eth Test form closes, and the CFM Eth Test (Create) form refreshes.

12 Configure the MEP Transmit LBM Information parameters:

- Data Size (octets)
- VLAN Priority

13 Click on the Apply button. The form displays additional buttons and tabs.

14 To execute the test, click on the Execute button.

15 Click on the Results tab to view the test results. See Procedure 32-44 for information about test results.

Procedure 32-10 To create and execute a CFM one-way delay diagnostic

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Ethernet CFM→CFM One Way Delay Test from the Create contextual menu. The CFM One Way Delay Test (Create) form opens.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- NM Administrative State

5 Click on the Select button beside the Global ID field to choose a global MEG. The Select Global MEG - CFM One Way Delay form opens.

6 Specify a search filter, if required, and click on the Search button. A list of global MEGs is displayed.

7 Select an entry and click on the OK button. The Select Global MEG - CFM One Way Delay form closes, and the CFM One Way Delay (Create) form displays the global MEG.

8 Click on the Select button beside the ID field to choose an originating MEP. The Select Originating MEP - CFM One Way Delay Test form opens.

9 Specify a search filter, if required, and click on the Search button. A list of MEPs is displayed.

10 Select a MEP in the list and click on the OK button. The Select Originating MEP - CFM One Way Delay Test form closes, and the CFM One Way Delay Test (Create) form displays the MEP information.

11 Perform one of the following:

a Select a MEP as the test destination. Perform the following steps.

i Click on the Select MEP button beside the Target MAC Address parameter to choose the destination MEP. The Select MEP - CFM One Way Delay form opens.

ii Select an entry and click on the OK button. The Select MEP - CFM One Way Delay form closes, and the CFM One Way Delay Test (Create) form refreshes.

b Select a MIP as the test destination. Perform the following steps.

i Click on the Select MIP button beside the Target MAC Address parameter to choose the destination MIP. The Select MIP - CFM One Way Delay form opens.

ii Select an entry and click on the OK button. The Select MIP - CFM One Way Delay form closes, and the CFM One Way Delay Test (Create) form refreshes.

c Select an unmanaged MEP as the test destination. Perform the following steps.

i Click on the Select Unmanaged MEP button beside the Target MAC Address parameter to select the destination MEP. The Select Unmanaged MEP - CFM One Way Delay form opens.

ii Select an entry and click on the OK button. The Select Unmanaged MEP - CFM One Way Delay form closes, and the CFM One Way Delay (Create) form refreshes.

12 Configure the Priority parameter in the MEP Transmit LBM Information panel.

13 Click on the Apply button. The form displays additional buttons and tabs.

14 To execute the test, click on the Execute button.

15 Click on the Results tab to view the test results. See Procedure 32-44 for information about test results.

Procedure 32-11 To create and execute a CFM two-way delay diagnostic



Note — The maximum number of continuous CFM two-way delay tests that can be executed is 300, provided that the SAA packet per second rate of 200 pps is not exceeded. The total number of continuous tests must share this maximum rate of 200 pps.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Ethernet CFM→CFM Two Way Delay Test from the Create contextual menu. The CFM Two Way Delay Test (Create) form opens.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- NM Administrative State
- NE Schedulable



Note — If the NE Schedulable parameter is enabled, two additional tabs are displayed for the form, Test Parameters and Results Configuration.

5 Click on the Select button beside the Global ID field to choose a global MEG. The Select Global MEG - CFM Two Way Delay form opens.

6 Specify a search filter, if required, and click on the Search button. A list of global MEGs is displayed.

7 Select an entry and click on the OK button. The Select Global MEG - CFM Two Way Delay form closes, and the CFM Two Way Delay (Create) form displays the global MEG.

8 Click on the Select button beside the ID field to choose an originating MEP. The Select Originating MEP - CFM Two Way Delay Test form opens.

9 Specify a search filter, if required, and click on the Search button. A list of MEPs is displayed.

10 Select a MEP in the list and click on the OK button. The Select Originating MEP - CFM Two Way Delay Test form closes, and the CFM Two Way Delay Test (Create) form displays the MEP information.

11 Perform one of the following:

a To select the test destination using the target's MAC Address, go to step 14.

b To select the test destination using the target's MEP ID, continue to step 12.



Note — MEP ID selection is only supported for OmniSwitch NEs. The NE Schedulable parameter must be enabled in step 4.

12 Enable the Enable Target MEP ID parameter.

13 Perform one of the following:

a Configure the Target MEP ID parameter.

b Select a MEP as the test destination. Perform the following steps.

i Click on the Select MEP button beside the Target MEP ID parameter to choose the destination MEP. The Select MEP - CFM Two Way Delay Test form opens.

ii Select an entry and click on the OK button. The Select MEP - CFM Two Way Delay Test form closes, and the CFM Two Way Delay Test (Create) form refreshes.

14 Perform one of the following:

a Select a MEP as the test destination. Perform the following steps.

i Click on the Select MEP button beside the Target MAC Address parameter to choose the destination MEP. The Select MEP - CFM Two Way Delay Test form opens.

ii Select an entry and click on the OK button. The Select MEP - CFM Two Way Delay Test form closes, and the CFM Two Way Delay Test (Create) form refreshes.

b Select a MIP as the test destination. Perform the following steps.

i Click on the Select MIP button beside the Target MAC Address parameter to choose the destination MIP. The Select MIP - CFM Two Way Delay Test form opens.

ii Select an entry and click on the OK button. The Select MIP - CFM Two Way Delay Test form closes, and the CFM Two Way Delay Test (Create) form refreshes.



Note — MIP selection is not supported for OmniSwitch NEs.

c Select an unmanaged MEP as the test destination. Perform the following steps.

i Click on the Select Unmanaged MEP button beside the Target MAC Address parameter to select the destination MEP. The Select Unmanaged MEP - CFM Two Way Delay Test form opens.

ii Select an entry and click on the OK button. The Select Unmanaged MEP - CFM Two Way Delay Test form closes, and the CFM Two Way Delay Test (Create) form refreshes.

15 If the NE Schedulable parameter was enabled in step 4 then go to step 18. Otherwise, go to step 16.

16 Configure the MEP Transmit DMM Information VLAN Priority parameter.

17 Go to step 20.

18 Click on the Test Parameters tab and configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Interval Units
- Packet Timeout (seconds)
- Forwarding Class
- Forwarding Profile
- Test Interval (minutes)
- Probe History
- Continuous Execution

The Probe History parameter is only configurable when the NE Schedulable parameter is enabled.

19 Click on the Results Configuration tab and configure the parameters:

- Test Failure Threshold
- Packet Failure Threshold
- Trap Generation
- Accounting Files
- Test Result Storage

The Trap Generation parameter is only configurable when the Accounting Files parameter is disabled.

The Test Result Storage parameter is only configurable when the Accounting Files parameter is enabled.

20 Click on the Apply button to save the changes.

21 To execute the test, click on the Execute button.

22 Click on the Results tab to view the test results. See Procedure 32-44 for information about test results.

Procedure 32-12 To create and execute a CFM single-ended loss diagnostic

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Ethernet CFM→CFM Single Ended Loss Test from the Create contextual menu. The CFM Single Ended Loss Test (Create) form opens.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- NM Administrative State

5 Click on the Select button beside the Global ID field to choose a global MEG. The Select Global MEG - CFM Single Ended Loss Test form opens.

6 Specify a search filter, if required, and click on the Search button. A list of global MEGs is displayed.

7 Select an entry and click on the OK button. The Select Global MEG - CFM Single Ended Loss Test form closes, and the CFM Single Ended Loss Test (Create) form displays the global MEG.

8 Click on the Select button beside the ID field to choose an originating MEP. The Select Originating MEP - CFM Single Ended Loss Test form opens.

9 Specify a search filter, if required, and click on the Search button. A list of MEPs is displayed.

10 Select a MEP in the list and click on the OK button. The Select Originating MEP - CFM Single Ended Loss Test form closes, and the CFM Single Ended Loss Test (Create) form displays the MEP information.

11 Choose a destination MEP:

i Click on the Select MEP button beside the Target MAC Address parameter. The Select MEP - CFM Single Ended Loss Test form opens.

ii Double-click on an entry in the list, or choose an entry and click on the OK button. The Select MEP - CFM Single Ended Loss Test form closes, and the CFM Single Ended Loss Test (Create) form refreshes.

12 Configure the following parameters in the MEP Transmit LMM Information panel:

- Priority
- Count
- Interval

13 Click on the Apply button. The form displays additional buttons and tabs.

14 To execute the test, click on the Execute button.

15 Click on the Results tab to view the test results. See Procedure 32-44 for information about test results.

Procedure 32-13 To create and execute a CFM two-way SLM (Synthetic Loss Measurement) diagnostic

Note — The maximum number of continuous CFM two-way SLM tests that can be executed is 300, provided that the SAA packet per second rate of 200 pps is not exceeded. The total number of continuous tests must share this maximum rate of 200 pps.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Ethernet CFM→CFM Two Way SLM from the Create contextual menu. The CFM Two Way SLM Test (Create) form opens.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- NM Administrative State
- NE Schedulable

Note — If the NE Schedulable parameter is enabled, two additional tabs are displayed for the form, Test Parameters and Results Configuration.

5 Click on the Select button beside the Global ID field to choose a global MEG. The Select Global MEG - CFM Two Way SLM Test form opens.

6 Specify a search filter, if required, and click on the Search button. A list of global MEGs is displayed.

7 Select an entry and click on the OK button. The Select Global MEG - CFM Two Way SLM Test form closes, and the CFM Two Way SLM Test (Create) form displays the global MEG.

8 Click on the Select button beside the ID field to choose an originating MEP. The Select Originating MEP - CFM Two Way SLM Test form opens.

9 Specify a search filter, if required, and click on the Search button. A list of MEPs is displayed.

10 Select a MEP in the list and click on the OK button. The Select Originating MEP - CFM Two Way SLM Test form closes, and the CFM Two Way SLM Test (Create) form displays the MEP information.

11 Perform one of the following:

a Select a MEP as the test destination. Perform the following steps.

i Click on the Select MEP button beside the Target MAC Address parameter to choose the destination MEP. The Select MEP - CFM Two Way SLM form opens.

ii Select an entry and click on the OK button. The Select MEP - CFM Two Way SLM form closes, and the CFM Two Way SLM Test (Create) form refreshes.

b Select a MIP as the test destination. Perform the following steps.

i Click on the Select MIP button beside the Target MAC Address parameter to choose the destination MIP. The Select MIP - CFM Two Way SLM form opens.

ii Select an entry and click on the OK button. The Select MIP - CFM Two Way SLM form closes, and the CFM Two Way SLM Test (Create) form refreshes.



Note — MIP selection is not supported on OmniSwitch NEs.

c Select an unmanaged MEP as the test destination. Perform the following steps.

i Click on the Select Unmanaged MEP button beside the Target MAC Address parameter to select the destination MEP. The Select Unmanaged MEP - Two Way SLM form opens.

ii Select an entry and click on the OK button. The Select Unmanaged MEP - CFM Two Way SLM form closes, and the CFM Two Way SLM (Create) form refreshes.

12 If the NE Schedulable parameter was enabled in step 4 then go to step 15. Otherwise, go to step 13.

13 In the MEP Transmit SLM Information panel, configure the following parameters:

- Priority
- Interval (seconds)
- Timeout (seconds)
- Data Size (octets)
- Send Count (packets)

14 Go to step 17.

15 Click on the Test Parameters tab and configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Interval Units
- Packet Timeout (seconds)
- Forwarding Class
- Forwarding Profile
- Probe History
- Size (octets)
- Continuous Execution

The Probe History parameter is only configurable when the NE Schedulable parameter is enabled.

16 Click on the Results Configuration tab and configure the parameters:

- Test Failure Threshold
- Packet Failure Threshold
- Trap Generation
- Accounting Files
- Test Result Storage

The Trap Generation parameter is only configurable when the Accounting Files parameter is disabled.

The Test Result Storage parameter is only configurable when the Accounting Files parameter is enabled.

17 Click on the Apply button to save the changes.

18 To execute the test, click on the Execute button.

19 Click on the Results tab to view the test results. See Procedure 32-44 for information about test results.

Procedure 32-14 To configure and run VPRN OAM diagnostics from a service

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Service Manager form opens.

2 Filter to list only the services on which you want to perform OAM diagnostics and click on the Search button.

3 Choose a service from the list and click on the Properties button. The Service (Edit) form opens.

4 Click on the Sites tab.

5 Choose a site or sites from the list and click on the Properties button. The Site (Edit) form opens.

6 Click on the Tests tab.

7 Configure and run a VPRN ping or VPRN trace OAM diagnostic.

a To configure and run a VPRN ping:

i Click on the VPRN Ping tab. A list of VPRN diagnostics appears.

ii Double-click on a row in the list to edit an existing test, or click on the Create button to create a new test. The VPRN ping form opens with the General tab displayed.

iii Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable

iv Click on the Select button to select a VPRN site. The Select VPRN Site - VPRN Ping form appears.

v Click on the Search button.

vi Select a VPRN site and click on the OK button. The Select VPRN Site - VPRN Ping form closes.

vii Click on the Test Parameters tab and configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Size (octets)
- Probe History
- Source IP Address
- Target IP Address
- Time To Live
- Reply Via Control Plane
- Forwarding Profile
- Forwarding Class

The Probe History parameter is only configurable when the NE Schedulable parameter is enabled.

viii Click on the Results Configuration tab and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Packet Failure Threshold
- Trap Generation

ix Click on the Apply button to save the changes.

x Confirm the action.

xi Click on the Execute button. A deployed test is created and run. Open the deployed test from the Deployed Tests tab to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

b To configure and run a VPRN trace:

i Click on the VPRN Trace tab. A list of VPRN trace diagnostics appears.

ii Double-click on a row in the list to edit an existing test, or click on the Create button to create a new test. The VPRN Trace (Create) form opens with the General tab displayed.

iii Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable

iv Click on the Select button to select a VPRN site. The Select VPRN Site - VPRN Trace form appears.

v Click on the Search button.

vi Select a VPRN site and click on the OK button. The Select VPRN Site - VPRN Trace form closes.

vii Click on the Test Parameters tab and configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Probe History
- Size (octets)
- Source IP Address
- Target IP Address
- Initial Time to Live
- Maximum Time to Live
- DiffServ Field
- Reply Via Control Plane
- Forwarding Profile
- Forwarding Class

The Probe History parameter is only configurable when the NE Schedulable parameter is enabled.

viii Click on the Results Configuration tab and configure the parameters:

- Probe History Size (rows)
- Maximum Failures
- Trap Generation

ix Click on the Apply button to save the changes.

x Confirm the action.

xi Choose the diagnostic from the list.

xii Click on the Execute button. A deployed test is created and run. Open the deployed test from the Deployed Tests tab to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

8 Configure and run an ICMP ping or ICMP trace OAM diagnostic.

a To configure and run ICMP ping:

i Click on the ICMP Ping tab. A list of ICMP diagnostics appears.

ii Double-click on a row in the list to edit an existing test, or click on the Create button to create a new test. The ICMP Ping form opens with the General tab displayed.

iii Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- Target Type
- From IP Address
- Target IP Address
- Next Hop Address

iv Click on the Test Parameters tab and configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Size (octets)
- Probe History
- Rapid
- Time To Live
- Data Pattern
- Positional Data Pattern
- DiffServ Field
- Egress Interface Index
- Bypass Routing
- Do Not Fragment

The Probe History parameter is only configurable when the NE Schedulable parameter is enabled.

v Click on the Results Configuration tab and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Packet Failure Threshold
- Trap Generation

vi Click on the Apply button to save the changes.

vii Click on the Execute button. A deployed test is created and run. Open the deployed test from the Deployed Tests tab to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

b To configure and run ICMP trace:

i Click on the ICMP Trace tab. A list of ICMP trace diagnostics appears.

ii Double-click on a row in the list to edit an existing test, or click on the Create button to create a new test. The ICMP Trace form opens with the General tab displayed.

iii Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- Target Type
- From IP Address
- Target IP Address

iv Click on the Test Parameters tab and configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Probe History
- Maximum Time to Live
- DiffServ Field
- Time To Wait (milliseconds)

The Probe History parameter is only configurable when the NE Schedulable parameter is enabled.

v Click on the Results Configuration tab and configure the parameters:

- Probe History Size (rows)
- Maximum Failures
- Trap Generation

vi Click on the Apply button to save the changes.

vii Choose the diagnostic from the list.

viii Click on the Execute button. A deployed test is created and run. Open the deployed test from the Deployed Tests tab to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

9 View the test results on the Results tab. The results depend on the type of test. See Procedure 32-44. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received



Note — Results of individually run ICMP Trace tests are viewed on the Results tab. The Results tab displays only the result of the last individually run ICMP Trace test, any previous individually run test results are overwritten.

Results from ICMP Trace tests that are scheduled or part of a test suite are also stored on the Results tab. The number of scheduled test results stored corresponds to the value configured in the Probe History Size (rows) parameter. Scheduled ICMP Trace test results do not overwrite individually run test results or previously run scheduled test results.

Procedure 32-15 To configure and run MAC populate OAM diagnostics

You can also perform the diagnostic from the Tests tab of a VPLS or Epipe VLL service form.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose L2 Service→Create MAC Populate from the Create contextual menu. The MAC Populate (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- Target Type
- Target MAC Address
- Send Via Control Plane
- Flood
- Force OAM
- Age (seconds)
- Service Name
- Name

When the Service Name parameter is configured, you can configure the Name parameter for the site.

5 Click on the Results Configuration tab and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Packet Failure Threshold
- Trap Generation

6 Click on the OK button to save the changes.

7 Choose the created test from the list of OAM diagnostics.

8 Click on the Execute button to start the MAC populate diagnostic. A deployed test is created and run. Open the deployed test from the Deployed Tests tab to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

9 View the test results on the Results tab. The results depend on the type of test. See Procedure 32-44. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 32-16 To configure and run MAC purge OAM diagnostics

You can also perform the diagnostic from the Test tab of a VPLS or an Epipe VLL.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose L2 Service→Create MAC Purge from the Create contextual menu. The MAC Purge (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- Target Type
- Target MAC Address
- Send Via Control Plane
- Inhibit Learning
- Flood
- Service Name
- Name

When the Service Name parameter is configured, you can configure the Name parameter for the site.

5 Click on the Results Configuration tab and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Packet Failure Threshold
- Trap Generation

6 Click on the OK button to save the changes.

7 Choose the created test from the list of OAM diagnostics.

8 Click on the Properties button.

9 Click on the Execute button to start the MAC purge diagnostic. A deployed test is created and run. Open the deployed test from the Deployed Tests tab to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

10 View the test results on the Results tab. The results depend on the type of test. See Procedure 32-44. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 32-17 To configure and run MAC ping OAM diagnostics

You can also perform the diagnostic from the Test tab of a VPLS or an Epipe VLL.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose L2 Service→ MAC Ping from the Create contextual menu. The MAC Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- Target Type
- Target MAC Address
- Source MAC Address
- Service Name
- Name

When the Service Name parameter is configured, you can configure the Name parameter for the site.

5 Click on the Test Parameters tab and configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Probe History
- Size (octets)
- Time To Live
- Forwarding Class
- Forwarding Profile
- Reply Control
- Control Plane

The Probe History parameter is only configurable when the NE Schedulable parameter is enabled.

6 Click on the Results Configuration tab and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Packet Failure Threshold
- Trap Generation

7 Click on the OK button to save the changes.

8 Choose the created test from the list of OAM diagnostics.

9 Click on the Properties button.

10 Click on the Execute button to start the MAC ping. A deployed test is created and run. Open the deployed test from the Deployed Tests tab to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

11 View the test results on the Results tab. The results depend on the type of test. See Procedure 32-44. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 32-18 To configure and run MAC trace OAM diagnostics

You can also perform the diagnostic from the Test tab of a VPLS or an Epipe VLL.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose L2 Service→Create MAC Trace from the Create contextual menu. The MAC Trace (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- Target Type
- Target MAC Address
- Source MAC Address
- Initial Time to Live
- Maximum Time to Live
- Service Name
- Name

When the Service Name parameter is configured, you can configure the Name parameter for the site.

5 Click on the Test Parameters tab and configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Probe History
- Forwarding Profile
- Forwarding Class

The Probe History parameter is only configurable when the NE Schedulable parameter is enabled.

6 Click on the Results Configuration tab and configure the parameters:

- Probe History Size (rows)
- Maximum Failures
- Trap Generation

7 Click on the Apply button to save the changes.

8 Choose the created test from the list of OAM diagnostics.

9 Click on the Execute button to start the MAC trace. A deployed test is created and run. Open the deployed test from the Deployed Tests tab to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

10 View the test results on the Results tab. The results depend on the type of test. See Procedure 32-44. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 32-19 To configure and run CPE ping OAM diagnostics

You can perform this test from the Test tab of a VPLS or on a VLL Epipe service provisioned over a VPLS PBB backbone. This test can also be added to the FirstRun/LastRun in a test suite.



Note 1 — You can also perform this diagnostic from:

- the Test tab→CPE Ping sub-tab of the required VPLS or VLL Epipe service
- the topology view of the required VPLS or VLL Epipe service

Note 2 — If the Epipe or the B-VPLS (in the case of PBB Epipe) uses SDP bindings, then the system configuration must be network chassis mode D compatible.

Note 3 — To run this test for a VLL Epipe over a VPLS PBB backbone, the NEs involved must be at IOM3 or above.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose L2 Service→Create CPE Ping from the Create contextual menu. The CPE Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- NM Administrative State
- NE Schedulable
- Service Name
- Name
- Destination Path Address
- Source IP Address
- Source MAC Address

When the Service Name parameter is configured, you can configure the Name parameter for the site.

The Source MAC Address parameter is only displayed and configurable when you are creating this test for a VPLS.

5 Click on the Test Parameters tab and configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Probe History
- VC's Label Time Live
- Send Via Control Plane
- Reply Via Control Plane
- Forwarding Profile
- Forwarding Class

The Probe History parameter is only configurable when the NE Schedulable parameter is enabled.

The Send Via Control Plane and Reply Via Control Plane parameters are only configurable for a VPLS.

6 Click on the Results Configuration tab and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Packet Failure Threshold
- Trap Generation

7 Click on the NM Thresholds tab to configure threshold-crossing alarms, as required.



Note — The NM Thresholds tab will only be displayed and configurable when the NE Schedulable parameter is not enabled.

Refer to Procedure 32-47 for details.

8 Click on the OK button to save the changes.

9 Click on the Search button to display the list of OAM diagnostics.

10 Double-click on the created test from the list of OAM diagnostics.

11 Click on the Execute button to start the CPE ping. A deployed test is created and run. Open the deployed test from the Deployed Tests tab to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

12 View the test results on the Results tab.

13 To display the test results, select the test from the CPE Ping Result list and click on the Properties button. The results depend on the type of test. See Procedure 32-44. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 32-20 To configure and run ANCP loopback diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose L2 Service→Create ANCP Loopback from the Create contextual menu. The ANCP Loopback (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State

5 Click on the Select button beside the System ID (Loopback Ip Address) parameter. The Select Originating Node - ANCP Loopback form opens.

6 Configure the filter criteria.

7 Click on the Search button.

8 Double-click on an entry in the list, or select an entry and click on the OK button. The Select Originating Node - ANCP Loopback form closes, and the ANCP Loopback (Create) form refreshes.

9 Click on the Test Parameters tab and perform one of the following steps.

   a Configure the ANCP loopback diagnostic for a subscriber ID.

      i Set the Target Type parameter to Subscriber Ident String.

      ii Configure the Subscriber Ident String parameter.

   b Configure the ANCP loopback diagnostic for an ANCP string.

      i Set the Target Type parameter to ANCP String.

      ii Configure the ANCP String parameter.

10 Configure the parameters:

- Count
- Timeout (seconds)

11 Click on the Results Configuration tab and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Packet Failure Threshold
- Trap Generation

12 Click on the Apply button to save changes.

13 Click on the Execute button to start the ANCP loopback diagnostic. A deployed test is created and run. Open the deployed test from the Deployed Tests tab to view its current state. When the test is complete you can view the results.

14 Click on the Results tab to view the test results.

15 Select the test from the ANCP Loopback Result list and click on the Properties button. The results depend on the type of test. See Procedure 32-44. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 32-21 To configure and run service site ping OAM diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Service→ Service Site Ping from the Create contextual menu. The Service Site Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- System ID (Loopback Ip Address)

5 Click on the Test Parameters tab and configure the parameters:

- Target IP Address
- Service ID
- Use Local Tunnel
- Use Remote Tunnel

When you set the target IP address, then choose a service ID, only service IDs from the selected site are available. When you set the Use Local Tunnel and Use Remote Tunnel parameters, the test becomes a ping that tests the service tunnel bindings between the service sites.

6 Click on the Results Configuration tab and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Packet Failure Threshold
- Trap Generation

7 Click on the OK button to save the changes.

8 Choose the created test from the list of OAM diagnostics and click on the Properties button.

9 Click on the Execute button to start the service site ping. A deployed test is created and run. Open the deployed test from the Deployed Tests tab to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

10 View the test results on the Results tab. The results depend on the type of test. See Procedure 32-44. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 32-22 To run the F5 OAM loopback diagnostic

This procedure is only supported on the 7705 SAR-M/ME when equipped with DSL modules.



Note — The parameters for the F5 OAM loopback test are only visible when the DSL module for the 7705 SAR-M/ME is connected to an ISAM device with the bonding type of ATM and the device is operationally up.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the port object where you want to configure an ethernet port. The path is Network→*NE*→Shelf→Card Slot→Daughter Card Slot→Port *n*/*n*/*n*.

3 Right-click on the Port icon and choose Properties. The Physical Port (Edit) form opens with the General tab displayed.

4 Click on the DSL tab.

5 Choose Active from the drop-down list for the F5 Oam Loopback parameter.

6 Click on the Apply button to save changes. A confirmation window opens.

7 Click on the Yes button. The loopback test is executed.

If the test was successfully executed, the F5 Oam Loopback Status field displays Pass and the F5 Oam Loopback Time field displays the time it took for the test to execute in milliseconds.

8 View the results from the F5 OAM Loopback test by opening a Telnet session on the NE, if required. See Procedure 11-2.

Procedure 32-23 To configure and run VCCV Ping OAM diagnostics

You can perform a VCCV Ping test from the Service Test Manager, as described in this procedure, but also from a VPLS/MVPLS or VLL service form, or from the service flat topology map.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Service→Create VCCV Ping from the Create contextual menu. The VCCV Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable

5 Click on the Select button in the First Spoke/Mesh SDP Binding panel. The Select First Spoke/Mesh SDP Binding - VCCV ping form appears.

6 Click on the Search button.

7 Select the required spoke or mesh SDP binding and click on the OK button. The Select First Spoke/Mesh SDP Binding - VCCV ping form closes.



Note — The selection of spoke bindings is applicable to both VPLS and VLL services, whereas mesh bindings are only applicable to VPLS and MVPLS. However, when creating this test for MVPLS and VPLS, the concept of downstream spoke SDP bindings does not apply.

8 If you are configuring this test for a VPLS, HVPLS, or MVPLS, then go to step 12.

9 Click on the Select button in the Downstream SDP Binding panel. The Select downstream spoke SDP Binding - VCCV ping form appears.

10 Click on the Search button.

11 Select the required downstream spoke SDP binding and click on the OK button. The Select downstream spoke SDP Binding - VCCV ping form closes.

12 Click on the Test Parameters tab and configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Probe History
- Size (octets)
- Forwarding Class
- Forwarding Profile
- Reply Type parameter

The Probe History parameter is only configurable when the NE Schedulable parameter is enabled.

13 Click on the Results Configuration tab and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Packet Failure Threshold
- Trap Generation

14 Click on the OK button to save the changes.

15 Choose the created test from the list of OAM diagnostics.

16 Click on the Execute button to start the VCCV ping. A deployed test is created and run. Open the deployed test from the Deployed Tests tab to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

17 View the test results on the Results tab. The results depend on the type of test. See Procedure 32-44. Result information includes:

- IP address of the destination and far-end device
- Time Last Response
- Number of Responses Received
- Response Time
- Loss indicator, a value of 0 indicates that the test packet was received and a value of 1 indicates that the test packet was lost

Procedure 32-24 To configure and run VCCV Trace OAM diagnostics

You can perform a VCCV Trace test from the Service Test Manager, as described in this procedure, but also from a VLL service form, or from the service flat topology map.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Service→Create VCCV Trace from the Create contextual menu. The VCCV Trace (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable

5 Click on the Select button in the First Spoke SDP Binding panel. The Select First Spoke SDP Binding - VCCV Trace form appears.

6 Click on the Search button.

7 Select the required spoke SDP binding and click on the OK button. The Select First Spoke SDP Binding - VCCV Trace form closes.

8 Configure the parameters:

- Initial Time to Live
- Maximum Time to Live

9 Click on the Test Parameters tab and configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Probe History
- Size (octets)
- Forwarding Class
- Forwarding Profile
- Reply Type parameter

The Probe History parameter is only configurable when the NE Schedulable parameter is enabled.

10 Click on the Results Configuration tab and configure the parameters:

- Probe History Size (rows)
- Maximum Failures
- Trap Generation

11 Click on the OK button to save the changes. The VCCV Trace (Create) form closes.

12 Click on the Test (Assurance) item in the Service Test Manager form and then click the Search button.

13 Choose the created test from the list of tests in the Test (Assurance) panel.

14 Click on the Execute button to start the VCCV Trace test. A deployed test is created and run.

15 Click on the Properties button. The VCCV Trace (Edit) form opens with the General tab displayed.

16 Click on the Deployed Tests tab to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

17 View the test results on the Results tab. The results depend on the type of test. See Procedure 32-44. Result information includes:

- information about the configuration test, including the configured parameter values
- number of probes to be issued
- time of last response
- source and response IP addresses
- number of hops
- probe responses from NEs in path

Procedure 32-25 To configure and run LSP or MPLS-TP LSP Ping OAM diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose MPLS→Create LSP Ping from the Create contextual menu. The LSP Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- Target Type
- Site ID
- IP Address
- Path ID
- Displayed Name
- Destination Path Address
- Next Hop Interface Name
- Next Hop Interface Address
- LDP Prefix
- LDP Prefix Length
- BGP Prefix
- BGP Prefix Length

The parameters in the Source IP Address, LDP, and Details panels can only be configured when the Target Type parameter is set to Any LSP and when the LDP Site ID is configured.

The BGP Prefix and BGP Prefix Length parameters can only be configured when the Target Type parameter is set to BGP LSP and when the BGP Site ID is configured.

5 If you set the Target Type parameter in step 4 to MPLS-TP LSP, perform the following:

i Click on the Select button in the MPLS-TP Site panel. The Select MPLS-TP Site - LSP Ping form opens with a list of MPLS-TP-enabled NEs.

ii Choose a site and click on the OK button. The Select MPLS-TP Site - LSP Ping form closes and the LSP Ping (Create) form refreshes with additional parameters.

iii Configure the Send Mode parameter.

iv Click on Select button in the MPLS-TP LSP panel. The Select MPLS-TP LSP Path - LSP Ping form opens.

v Choose an MPLS-TP path and click on the OK button.

vi Configure the parameters:

- MPLS-TP LSP Path Type
- Destination Global ID
- Destination IP Address

You can configure the Destination Global ID and Destination IP Address parameters with the LER or intermediate NEs (LSRs).

6 Click on the Test Parameters tab and configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Probe History
- Size (octets)
- Time To Live
- Forwarding Class
- Forwarding Profile

When you set the target IP address, then choose a service ID, only service IDs from the selected site are available.

The Probe History parameter is only configurable when the NE Schedulable parameter is enabled.

7 Click on the Results Configuration tab and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Packet Failure Threshold
- Trap Generation

8 Click on the OK button to save the changes. The Service Test Manager form opens.

9 Double-click on the created test from the list of OAM diagnostics.

10 Click on the Execute button to start the LSP ping. A deployed test is created and run. Open the deployed test from the Deployed Tests tab to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

11 View the test results on the Results tab. The results depend on the type of test. See Procedure 32-44. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 32-26 To configure and run LSP or MPLS-TP LSP Trace OAM diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose MPLS→Create LSP Trace from the Create contextual menu. The LSP Trace (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- Target Type
- Site ID
- IP Address
- LDP Prefix
- LDP Prefix Length
- BGP Prefix
- BGP Prefix Length
- Destination Path Address
- Packet Failure Threshold
- Next Hop Interface Address

The parameters in the Source IP Address, LDP, and Details panels can only be configured when the Target Type parameter is set to Any LSP and when the LDP Site ID is configured.

The BGP Prefix and BGP Prefix Length parameters can only be configured when the Target Type parameter is set to BGP LSP and when the BGP Site ID is configured.

5 If you set the Target Type parameter in step 4 to MPLS-TP LSP, perform the following:

i Click on the Select button in the MPLS-TP Site panel. The Select MPLS-TP Site - LSP Trace form opens with a list of MPLS-TP-enabled NEs.

ii Choose a site and click on the OK button. The Select MPLS-TP Site - LSP Trace form closes and the LSP Trace (Create) form refreshes with additional parameters.

iii Configure the Send Mode parameter.

iv Click on Select button in the MPLS-TP LSP panel. The Select MPLS-TP LSP Path - LSP Trace form opens.

v Choose an MPLS-TP path and click on the OK button.

vi Configure the MPLS-TP LSP Path Type parameter.

6 Click on the Test Parameters tab and configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Probe History
- Size (octets)
- Initial Time to Live
- Maximum Time to Live
- Forwarding Class
- Forwarding Profile

When you set the target IP address, then choose a service ID, only service IDs from the selected site are available.

The Probe History parameter is only configurable when the NE Schedulable parameter is enabled.

7 Click on the Results Configuration tab and configure the parameters:

- Probe History Size (rows)
- Maximum Failures
- Trap Generation

8 Click on the OK button to save the changes. The Service Test Manager form opens.

9 Choose the created test from the list of OAM diagnostics and click on the Properties button.

10 Click on the Execute button to start the LSP trace. A deployed test is created and run. Open the deployed test to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

11 View the test results on the Results tab. The results depend on the type of test. See Procedure 32-44. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 32-27 To configure and run P2MP LSP Ping OAM diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose MPLS→Create P2MP LSP Ping from the Create contextual menu. The P2MP LSP Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- NM Administrative State
- Target Type

5 Perform one of the following:

a If you selected P2MP RSVP as your Target Type, then:

i Click the Select button in the P2MP Dynamic LSP panel to choose the P2MP Dynamic LSP you want to test. The Select P2MP Dynamic LSP - P2MP LSP Ping form is displayed.

ii Click the Search button.

iii Select the required P2MP Dynamic LSP and click OK.

The Select P2MP Dynamic LSP - P2MP LSP Ping form closes and the P2MP LSP Ping (Create) form is refreshed to show your selection.

iv Click the Select button in the P2MP Instance panel to choose the P2MP Instance you want to test. The Select P2MP Instance - P2MP LSP Ping form is displayed.

v Select the required P2MP Instance and click OK.

The Select P2MP Instance - P2MP LSP Ping form closes and the P2MP LSP Ping (Create) form is refreshed to show your selection.

vi Configure the Select All S2L Paths parameter.

If you enabled the parameter, go to step 6.

vii Click on the S2L Paths tab.

viii Click the Add button. The Add form is displayed.

ix Click the Search button. A list of available S2L paths is displayed.

x Select the S2L paths that you want to test (up to a maximum of five) and click OK. The Add form closes and the selected S2L paths are displayed in the list.

xi Go to step 6.

b If you selected P2MP mLDP as your Target Type, then:



Note — For the test to execute successfully, ensure the following:

- The LDP protocol must be enabled on all NEs between the source and destination, including any intermediate NEs.
- LDP interfaces must be in place between the source and destination NEs.
- LDP interfaces must be up, and the Multicast Forwarding parameter must be enabled on each interface. This also applies to all intermediate NEs. Refer to Procedure 23-14 for information on configuring LDP interfaces.

i Click the Select button in the P2MP LDP panel to choose the P2MP ID you want to test. The Select P2MP ID - P2MP LSP Ping form is displayed.

ii Click the Search button. Only root NEs are listed.

iii Select the required P2MP ID and click OK.

The Select P2MP ID - P2MP LSP Ping form closes and the P2MP LSP Ping (Create) form is refreshed to show your selection.

iv Click on the LDP Leaf Addresses tab.

v Click the Add button. The Add form is displayed.

vi Click the Search button. A list of available leaf NEs is displayed.

vii Select the leaf NEs that you want to test (up to a maximum of five) and click OK.

The Add form closes and the selected leaf NEs are displayed in the list.

6 Click on the Test Parameters tab and configure the parameters:

- Packet Timeout (seconds)
- Packet Interval (seconds)
- Size (octets)
- Time To Live
- Forwarding Class
- Forwarding Profile

The Time To Live parameter is only displayed if you selected P2MP RSVP as your Target Type.

7 Click on the Results Configuration tab and configure the parameters:

- Test Failure Threshold
- Packet Failure Threshold
- Trap Generation

8 Click on the NM Thresholds tab to configure threshold-crossing alarms, as required.

Refer to Procedure 32-47 for details.

9 Click on the OK button to save the changes. The Service Test Manager form opens.

10 Choose the created test from the list of OAM diagnostics and click on the Properties button.

The P2MP LSP Ping (Edit) form opens, with the General tab displayed.

11 Click on the Execute button to start the P2MP LSP ping. A deployed test is created and run. Open the deployed test to view its current state. When the test is complete, the deployed test is removed, and you can view the results.



Note — When this test is performed on an existing Point-to-Multipoint LSP, up to five S2L paths (for a P2MP RSVP target type) or five LDP leaf addresses (for a P2MP mLDP target type) can be selected. If none are selected, all available paths or addresses up to the limit of five will be pinged.

12 Click on the Results tab in the P2MP LSP Ping (Edit) form.

The Results tab will show an entry for each S2L path (RSVP) or leaf address (mLDP) tested.

13 Select the test from the list and click on Properties. The P2MP LSP Ping Packet Result form opens, with the General tab displayed.

The General tab displays the test parameters you configured, along with time the test was executed, its status, and the following test information:

- Number of Packets Sent
- Packet Timeouts
- Number of Responses Received
- Number of Packets Lost
- Loss Percentage
- Last Good Packet Time



Note — The test results depend on the type of test you run. Refer to Procedure 32-44 for more information.

14 Click on the Details tab.

15 View the test results for the:

- Round Trip Time
- Outbound One Way Time
- Inbound One Way Time

16 Click on the Response Packets tab.

17 Select a response packet from the list and click on Properties. The P2MP LSP Ping Packet Result form opens.



Note — The test results depend on the type of test you run. Refer to Procedure 32-44 for more information.

18 View details on the response packet, including:

- Status
- Round-Trip Time
- Response sequence

19 Repeat steps 13 to 18 for all tested S2L paths (RSVP) or leaf addresses (mLDP).



Note — Refer to the Service assurance test management and configuration in Section 32.1 and to Chapter 77 for more information on viewing test results.

Procedure 32-28 To configure and run P2MP LSP Trace OAM diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose MPLS→Create P2MP LSP Trace from the Create contextual menu. The P2MP LSP Trace (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- NM Administrative State

5 Click the Select button in the P2MP Dynamic Lsp panel to choose the P2MP Dynamic LSP you want to test.

6 Click the Select button in the P2MP Instance panel to choose the P2MP Instance you want to test.

7 Click the Select button in the S2L Destination Address panel to choose the S2L Destination Address you want to test.

8 Click on the Test Parameters tab and configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Size (octets)
- Initial Time to Live
- Maximum Time to Live
- Forwarding Class
- Forwarding Profile

9 Click on the Results Configuration tab and configure the parameters:

- Maximum Failures
- Trap Generation

10 Click on the NM Thresholds tab to configure threshold-crossing alarms, as required.

Refer to Procedure 32-47 for details.

11 Click on the OK button to save the changes. The Service Test Manager form opens.

12 Choose the created test from the list of OAM diagnostics and click on the Properties button.

The P2MP LSP Trace (Edit) form opens, with the General tab displayed.

13 Click on the Execute button to start the P2MP LSP trace. A deployed test is created and run. Open the deployed test to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

14 Click on the Results tab.

15 Select the test from the list and click on Properties. The P2MP LSP Trace Result form opens, with the General tab displayed.

The General tab displays the test parameters you configured, along with time the test was executed and its status.

Note — The test results depend on the type of test you run. Refer to Procedure 32-44 for more information.

16 Click on the Hops and Probes tab.

A tree view of the Hops and Probes associated with this test is provided.

17 Right-click on a Hop from the tree view and click on Properties.

The P2MP LSP Trace Hop (Edit) form is displayed, showing the General tab.

18 View the test results for the:

- Response Probe
- Round Trip Details
- Outbound One Way Trip Details
- Inbound One Way Trip Details

19 Right-click on a Probe from the tree view and click on Properties.

The P2MP LSP Trace Probe (Edit) form is displayed, showing the General tab.

20 View details on the probe, including:

- Response Probe
- LSP Details

21 Repeat this test for all required S2L paths. The test only evaluates one S2L path per execution.

Note — Refer to the Service assurance test management and configuration in Section 32.1 and to Chapter 77 for more information on viewing test results.

Procedure 32-29 To configure and run LDP Tree Trace OAM diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button. The test options are displayed in a drop-down menu.

3 Choose MPLS→Create LDP Tree Trace from the Create contextual menu. The LDP Tree Trace (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- Site ID
- LDP Prefix
- LDP Prefix Length

5 Click on the Test Parameters tab and configure the parameters:

- Maximum Time to Live
- Timeout (seconds)
- Retry Counter
- Forwarding Class
- Profile
- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)

6 Click on the Results Configuration tab and configure the parameters:

- Probe History Size (rows)
- Maximum Failures
- Trap Generation

7 Click on the OK button to save the changes. The Service Test Manager form opens.

8 Choose the created test from the list of OAM diagnostics and click on the Properties button.

9 Click on the Execute button to start the LDP tree trace. A deployed test is created and run. Open the deployed test to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

10 Click on the Results tab. A list of LDP tree trace tests appears.

11 Choose a LDP tree trace from the list and click on the Properties button.

12 View the test results. The results depend on the type of test. See Procedure 32-44.

Procedure 32-30 To configure and run multicast router information OAM diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Multicast→Create Mrinfo from the Create contextual menu. The mrinfo (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- Target Type
- Site ID

5 Click on the Results Configuration tab and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Packet Failure Threshold
- Trap Generation

6 Click on the Select button to choose a PIM interface. The Select PIM Interface form opens.

7 Select a PIM interface in the list and click on the OK button. The Select PIM Interface form closes, and the interface information is displayed on the mrinfo (Create) form.

8 Click on the OK button to save the changes.

9 Choose the created test from the list of OAM diagnostics.

10 Click on the Execute button to start the diagnostic request for multicast router information. A deployed test is created and run. Open the deployed test to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

11 View the test results on the Results tab. The results depend on the type of test. See Procedure 32-44.

Procedure 32-31 To configure and run multicast trace OAM diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Multicast→Create Mtrace from the Create contextual menu. The mtrace (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- Target Type
- Site ID
- Source Address
- Destination Address
- Response Address

5 Click on the Test Parameters tab and configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Initial Time to Live
- Maximum Number of Hops

When you set the target IP address, then choose a service ID, only service IDs from the selected site are available.

6 Click on the Results Configuration tab and configure the parameters:

- Probe History Size (rows)
- Maximum Failures
- Trap Generation

7 Click on the OK button to save the changes.

8 Choose the created test from the list of OAM diagnostics.

9 Click on the Execute button to start the multicast trace. A deployed test is created and run. Open the deployed test to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

10 View the test results on the Results tab. The results depend on the type of test. See Procedure 32-44.

Procedure 32-32 To configure and run multicast FIB ping OAM diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Multicast→Create Mfib Ping from the Create contextual menu. The MFIB Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- Service Name
- Multicast Source
- Multicast Group
- Name

When the Service Name parameter is configured, you can configure the Name parameter for the site.

5 Click on the Test Parameters tab and configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Size (octets)
- Time To Live
- Timeout (seconds)
- Reply Via Control Plane

When you set the target IP address, then choose a service ID, only service IDs from the selected site are available.

6 Click on the Results Configuration tab and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Packet Failure Threshold
- Trap Generation

7 Click on the OK button to save the changes.

8 Choose the created test from the list of OAM diagnostics.

9 Click on the Execute button to start the multicast FIB ping. A deployed test is created and run. Open the deployed test to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

10 View the test results on the Results tab. The results depend on the type of test. See Procedure 32-44.

Procedure 32-33 To configure and run an ATM OAM ping

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose L1/L2→Create ATM Ping from the Create contextual menu. The ATM Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- ATM Interface ID

5 Click on the Test Parameters tab and configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Loopback Location (hex)
- Destination Type

6 Click on the Results Configuration tab and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Packet Failure Threshold
- Trap Generation

7 Click on the Apply button to save the settings. A confirmation window opens.

8 Click on the Yes button.

9 Choose the created test from the list of OAM diagnostics.

10 Click on the Execute button to start the ATM ping. A deployed test is created and run. Open the deployed test from the Deployed Tests tab to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

11 View the test results on the Results tab. The results depend on the type of test. See Procedure 32-44. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

12 To configure another ATM OAM ping, click on the Clear button and repeat steps 5 to 11. Otherwise, go to step 13.

13 Click on the Cancel button to close the form.

Procedure 32-34 To configure an ATM OAM loopback

ATM OAM loopback settings are configured globally on supported devices. However, a loopback must be enabled on an IES or VPRN SAP.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure an ATM OAM loopback and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the ATM tab.

4 Configure the parameters:

- ATM OAM Loopback Location ID
- ATM OAM Loopback Period
- Number of Tries for Up State
- Number of Tries for Down State

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Network Element (Edit) form closes.

Procedure 32-35 To configure and run an ICMP ping

You can also perform an ICMP ping from the Test tab of a VPRN or EIS service configuration form.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose ICMP→ ICMP Ping from the Create contextual menu. The ICMP Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- Target Type
- System ID (Loopback Ip Address)
- From IP Address
- Source IP Address
- Target IP Address
- Next Hop Address

5 Click on the Test Parameters tab and configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Probe History
- Size (octets)
- Rapid
- Time To Live
- Data Pattern
- Positional Data Pattern
- DiffServ Field
- Egress Interface Index
- Bypass Routing
- Do Not Fragment
- Forwarding Class
- Forwarding Profile

The Probe History parameter is only configurable when the NE Schedulable parameter is enabled.

6 Click on the Results Configuration tab and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Packet Failure Threshold
- Trap Generation

7 Click on the Apply button to save the settings.

8 Click on the Execute button to start the ICMP ping. A deployed test is created and run. Open the deployed test from the Deployed Tests tab to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

9 View the test results on the Results tab. The results depend on the type of test. See Procedure 32-44. Result information includes:

- Average Round-Trip Time
- Maximum Round-Trip Time
- Minimum Round-Trip Time
- Round-Trip Jitter

10 To configure another ICMP ping, click on the Clear button and repeat steps 5 to 9. Otherwise, go to step 11.

11 Click on the Cancel button to close the form.

Procedure 32-36 To configure and run an ICMP trace

You can also perform an ICMP trace from the Test tab of a VPRN or EIS.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose ICMP→Create ICMP Trace from the Create contextual menu. The ICMP Trace (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- Target Type
- System ID (Loopback Ip Address)
- From IP Address
- Source IP Address
- Target IP Address

5 Click on the Test Parameters tab and configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Probe History
- Maximum Time to Live
- DiffServ Field
- Time To Wait (milliseconds)

The Probe History parameter is only configurable when the NE Schedulable parameter is enabled.

6 Click on the Results Configuration tab and configure the parameters:

- Probe History Size (rows)
- Maximum Failures
- Trap Generation

7 Click on the Apply button to save the settings.

8 Click on the Execute button to start the ICMP trace. A deployed test is created and run. Open the deployed test from the Deployed Tests tab to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

9 View the test results on the Results tab. The results depend on the type of test. See Procedure 32-44. Result information includes:

- Current Hop Count
- Current Probe Count
- Minimum Round-Trip Time
- Round-Trip Jitter



Note — Results of individually run ICMP Trace tests are viewed on the Results tab. The Results tab displays only the result of the last individually run ICMP Trace test, any previous individually run test results are overwritten.

Results from ICMP Trace tests that are scheduled or part of a test suite are also stored on the Results tab. The number of scheduled test results stored corresponds to the value configured in the Probe History Size (rows) parameter. Scheduled ICMP Trace test results do not overwrite individually run test results or previously run scheduled test results.

10 To configure another ICMP trace, click on the Clear button and repeat steps 5 to 9. Otherwise, go to step 11.

11 Click on the Cancel button to close the form.

Procedure 32-37 To configure and run a DNS ping

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose ICMP→Create DNS Ping from the Create contextual menu. The DNS Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- Target Type
- System ID (Loopback Ip Address)
- From IP Address
- Source IP Address
- DNS Server Type
- DNS Name
- DNS Server Address

5 Click on the Test Parameters tab and configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Probe History

The Probe History parameter is only configurable when the NE Schedulable parameter is enabled.

6 Click on the Results Configuration tab and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Packet Failure Threshold
- Trap Generation

7 Click on the Apply button to save the settings.

8 Click on the Execute button to start the DNS ping. A deployed test is created and run. Open the deployed test from the Deployed Tests tab to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

9 View the test results on the Results tab. The results depend on the type of test. See Procedure 32-44. Result information includes:

- Average Round-Trip Time
- Maximum Round-Trip Time
- Minimum Round-Trip Time
- Round-Trip Jitter
- Sum of Squares Round-Trip Time

10 To configure another DNS ping, click on the Clear button and repeat steps 5 to 9. Otherwise, go to step 11.

11 Click on the Cancel button to close the form.

Procedure 32-38 To create an OmniSwitch OAM CLI script



Warning — Scripts that are not correctly created or applied can cause serious damage to the network. Alcatel-Lucent recommends that system administrators clearly define user responsibilities for CLI script usage, and ensure that scripts are verified and validated before they are executed on devices in a live network.

Perform this procedure to create an OmniSwitch OAM CLI script using the sample scripts in Code 32-1 and Code 32-2.

1 Choose Tools→Scripts from the 5620 SAM main menu. The Scripts form opens.

2 Choose CLI Script (Scripting) from the object drop-down list and click on the Create button. The CLI Script (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Auto-Assign ID
- Script ID
- Name
- Description
- Type
- Use Latest Version
- Starting Point
- Continue On Command Failure
- Content Type

Enable the Use Latest Version parameter to associate all of the targets of the script with the latest version of the CLI script.

You must set the Content Type parameter to Velocity.

4 Perform the following steps to specify the script target types.

i Click on the Add button in the NE Types panel. The Select Property - CLI Script form opens.

ii Select one or more OmniSwitch NE types in the list and click on the OK button. The Select Property - CLI Script form closes, and the NE types are listed on the CLI Script (Create) form.

5 Click on the Apply button to apply the configuration.

6 Click on the Versions tab.

7 Create the script by clicking on the Create button. The Script Editor *script_name* form opens.

8 Create the CLI script text by performing one of the following steps.

a Import an existing text file with a CLI script. You can create a text file by copying and pasting the text from the sample OmniSwitch ping shown in Code 32-1 or the sample traceroute script shown in Code 32-2 into a text editor.

i Choose File→Import from the Editor menu. The Import dialog box appears.

ii Choose the file to be imported and click on the Import button. The script appears in the Script Editor workspace.

iii Modify the script as required.

b Enter or copy and paste the CLI script text from the sample OmniSwitch ping shown in Code 32-1 or the sample traceroute script shown in Code 32-2 into the Script Editor workspace.



The following ping and traceroute scripts are sample CLI scripts that can be used to run ping and traceroute tests. See the *5620 SAM Scripts and Templates Developer Guide* for information about creating, configuring, and using scripts.

Code 32-1: Sample OmniSwitch OAM ping script

```
<velocityProperties>
  <tab><name>General</name><tooltip>The general tab</tooltip>
    <group><name>General</name><tooltip>The general group</tooltip>
      <property>
        <name>ip_address</name>
        <uiName>IP Address:</uiName>
        <tooltip>IP address of the system to ping (IPv4
xxx.xxx.xxx.xxx)</tooltip>
        <type>String</type>
        <default>0.0.0.0</default>
        <uiOrder>1</uiOrder>
        <required>true</required>
      </property>
      <property>
        <name>count</name>
        <uiName>Count:</uiName>
        <tooltip>Number of frames to be transmitted</tooltip>
        <type>Integer</type>
        <default>6</default>
        <uiOrder>2</uiOrder>
        <required>true</required>
      </property>
      <property>
        <name>packed_size</name>
        <uiName>Packet Size:</uiName>
        <tooltip>Size of the data portion of the packet sent for this
ping, in bytes</tooltip>
        <type>Integer</type>
        <default>64</default>
        <required>true</required>
```

```
        <uiOrder>3</uiOrder>
        <min>1</min>
        <max>60000</max>
      </property>
      <property>
        <name>interval</name>
        <uiName>Interval (seconds):</uiName>
        <tooltip>Polling interval</tooltip>
        <type>Integer</type>
        <uiOrder>4</uiOrder>
        <default>1</default>
        <min>1</min>
        <max>10000</max>
      </property>
      <property>
        <name>timeout</name>
        <uiName>Timeout (seconds):</uiName>
        <tooltip>Number of seconds the program will wait for a
response before timing out</tooltip>
        <type>Integer</type>
        <uiOrder>5</uiOrder>
        <default>5</default>
        <min>1</min>
        <max>10000</max>
      </property>
    </group>
  </tab>
</velocityProperties>

ping $ip_address count $count size $packed_size interval $interval
timeout $timeout
```

Code 32-2: Sample OmniSwitch traceroute script

```
<velocityProperties>
  <tab><name>General</name><tooltip>The general tab</tooltip>
    <group><name>General</name><tooltip>The general group</tooltip>
      <property>
        <name>ip_address</name>
        <uiName>IP Address:</uiName>
        <tooltip>IP address of the host whose route you want to trace.
(IPv4 xxx.xxx.xxx.xxx)</tooltip>
        <type>String</type>
        <default>0.0.0.0</default>
        <uiOrder>1</uiOrder>
        <required>true</required>
      </property>
      <property>
        <name>maxHopValue</name>
        <uiName>Maximum Hop:</uiName>
        <tooltip>Maximum hop count for the trace</tooltip>
        <type>Integer</type>
        <default>5</default>
        <uiOrder>2</uiOrder>
        <required>true</required>
      </property>
    </group>
```

```
  </tab>
</velocityProperties>

traceroute $ip_address max-hop $maxHopValue
```

9 Perform one of the following.

a Save the script to the Scripts tool.

i Choose File→Save from the Editor menu or click on the Save button. The Comment form opens.

ii Configure the parameters:

- Network Element Version Information
- Bundle ID

iii Click on the OK button.

b Export the script to a local or network text file.

i Choose File→Export from the Editor menu, or click on the Export button. A dialog box appears and prompts you to choose a file storage location in the network.

ii Scroll to the location in which you want to save the text file, and enter a filename in the appropriate field.

iii Click on the Export button. The script version text file is saved in the specified location.

10 Choose File→Close from the Editor menu. The Script Editor form closes, and the CLI Script (Edit) form reappears with the Version tab displayed. The new version of the script appears in the list.

11 Close the CLI Script (Edit) form.

12 Close the Scripts list form.

See procedures 32-40 and 32-41 for information about configuring and running OmniSwitch ping and traceroute OAM scripts.

Procedure 32-39 To configure an advanced loopback test on an OmniSwitch port



Note 1 — Only one test profile per port can be created, up to a maximum of 8 ports on an NE.

Note 2 — The test profile cannot be created on a port that is part of a LAG.

1 Choose Equipment from the navigation tree. The navigation tree displays the Equipment view.

2 Expand the OmniSwitch NEs icon.

3 Right-click on the device where you want to configure an advanced loopback test and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

5 Expand to the port level and click on a port object. The Physical Port (Edit) form opens with the General tab displayed.

6 Click on the Advanced Loopback tab. Click on the Create button. The AOS Advanced Loopback (Create) form appears.

7 Configure the parameters:

- Test Name
- Source MAC Address
- Destination MAC Address
- VLAN
- Traffic Type
- SAP Id (OS 6250 and OS 6450 only, see Note 1 and Note 2)



Note 1 — For OS 6250 and OS 6450 NEs, when the Traffic Type parameter value is set to Outward, the user can specify the SAP Id, provided the SAP Id already exists on the NE.

Note 2 — If a loopback profile is created with the Traffic Type parameter value set to Outward, the SAP Id parameter will be provided with the default value of 0. If the loopback profile is created with a SAP Id, then the SAP Id must exist on the NE.

8 Click on the OK button. A dialog box appears.

9 Click on the OK button. The AOS Advanced Loopback (Create) form closes.

10 Choose a test entry on the Physical Port (Edit) form. Click on the Apply button. A dialog box appears.

11 Click on the Yes button.

12 Choose a test entry on the Physical Port (Edit) form. Click on the Properties button.

13 The AOS Advanced Loopback (Edit) form opens. Configure the Status parameter.

14 Click on the OK button. The AOS Advanced Loopback (Edit) form closes.

15 Click on the OK button of the Physical Port (Edit) form. A dialog box appears.

16 Click on the Yes button. The Physical Port (Edit) form closes.

Procedure 32-40 To configure and run an OmniSwitch OAM ping



Warning — Scripts that are not correctly created or applied can cause serious damage to the network. Alcatel-Lucent recommends that system administrators clearly define user responsibilities for CLI script usage, and ensure that scripts are verified and validated before they are executed on devices in a live network.

The following procedure describes how to configure and run an OmniSwitch ping test using the script created using Procedure 32-38.

1 Ensure that the mediation policy for each OmniSwitch target is configured with the correct user name and password for CLI communication. See Procedure 10-4.

2 Choose Tools→Scripts from the 5620 SAM main menu. The Scripts form opens.

3 Choose CLI Script (script) from the object drop-down list.

4 Configure the filter criteria. A list of scripts appears at the bottom of the Scripts form.

5 Double-click on the OmniSwitch ping script that you created using Procedure 32-38. The CLI Script (Edit) form opens with the General tab displayed.

6 Click on the Targets tab.

7 Click on the Create button. The Target Configuration form opens.

8 Click on the Create button. The Select Network Elements form opens.

9 Choose one or more OmniSwitch devices and click on the OK button. The Select Network Elements form closes, and the OmniSwitch NEs are listed on the Target Configuration form.

10 Configure the test parameters.

i Choose a target from the Target List panel.

ii Configure the parameters:

- IP Address
- Count
- Packet Size (octets)
- Interval (seconds)
- Timeout

iii Click on the Apply To Selected button.

iv Repeat steps 10i to 10iii to configure additional targets, if required.

v Click on the OK button to close the Target Configuration form. The CLI Script (Edit) form opens with the Targets tab displayed.

11 To run the script on specified targets, choose one or more entries from the list.

12 Click on the Execute button. The results of the test appear in the form.

13 Perform one of the following to view the results of the scripts:

a Choose a target from the list. The results of the script that was run on the specified target appears in the panel below the list.

i Click on the Save Result button to save the results to the result manager. A dialog box appears. Click on the OK button.



Note — You can save the results of multiple scripts to the result manager simultaneously; choose the entries in the list and click on the Save Result button.

ii Export the results to a local or network text file.

iii Click on the Export button. A dialog box appears and prompts you to choose a file storage location on the network.

iv Scroll to the location in which you want to save the text file, and enter a filename in the appropriate field.

v Click on the Export button. The results text file is saved in the specified location.

b Choose one or more entries from the list and click on the View Selected button. The View Selected form opens and displays the results of the script. The results for each target are separated by a comment that indicates the script version, associated target, script status, run time and date, and script parameters.

i Export the results of the script to a local or network text file. Choose File→Export from the Editor menu, or click on the Export button. A dialog box appears and prompts you to choose a file storage location in the network. Scroll to the location in which you want to save the text file, and enter a filename in the appropriate field. Click on the Export button. The results text file is saved in the specified location.

ii Choose File→Close from the View Selected form to close the View Selected form.

14 Click on the OK button or Cancel button to close the CLI Script (Edit) form.

15 Close the Scripts form.

Procedure 32-41 To configure and run an OmniSwitch OAM traceroute



Warning — Scripts that are not correctly created or applied can cause serious damage to the network. Alcatel-Lucent recommends that system administrators clearly define user responsibilities for CLI script usage, and ensure that scripts are verified and validated before they are executed on devices in a live network.

The following procedure describes how to configure and run an OmniSwitch traceroute using the script created using Procedure 32-38.

1 Ensure that the mediation policy for each OmniSwitch target is configured with the correct user name and password for CLI communication. See Procedure 10-4.

2 Choose Tools→Scripts from the 5620 SAM main menu. The Scripts list form opens.

3 Choose CLI Script (script) from the object drop-down list.

4 Configure the filter criteria. A list of scripts appears at the bottom of the Scripts form.

5 Double-click on the OmniSwitch traceroute script that you created using Procedure 32-38. The CLI Script (Edit) form opens with the General tab displayed.

6 Click on the Targets tab.

7 Click on the Add button. The Target Configuration form opens.

8 Click on the Add button in the target list to add an OmniSwitch to the list. The Select Network Elements form opens with a list of OmniSwitch NEs.

9 Choose one or more OmniSwitch NEs and click on the OK button. The Select Network Elements form closes, and the OmniSwitch NEs appear in the target list panel of the Target Configuration form.

10 Configure the test parameters.

   i Choose a target from the Target List panel.

   ii Configure the parameters:

   - IP Address
   - Maximum Hop

   iii Click on the Apply To Selected button.

   iv Repeat steps 10i to 10iii to configure additional targets.

   v Click on the OK button to close the Target Configuration form. The CLI Script (Edit) appears with the Targets tab displayed.

11 To run the script on the specified targets, choose one or more entries from the list.

12 Click on the Execute button. The test results appear.

13 Perform one of the following to view the results of the scripts:

a Choose a target from the list. The results of the script that was run on the specified target appears in the panel below the list.

i Click on the Save Result button to save the results to the result manager. A dialog box appears. Click on the OK button.



Note — You can save the results of multiple scripts to the result manager simultaneously; choose the entries in the list and click on the Save Result button.

ii Export the results to a local or network text file.

iii Click on the Export button. A dialog box appears and prompts you to choose a file storage location on the network.

iv Scroll to the location in which you want to save the text file, and enter a filename in the appropriate field.

v Click on the Export button. The results text file is saved in the specified location.

b Choose one or more entries from the list and click on the View Selected button. The View Selected form opens and displays the results of the script. The results for each target are separated by a comment that indicates the script version, associated target, script status, run time and date, and script parameters.

i Export the results of the script to a local or network text file. Choose File→Export from the Editor menu, or click on the Export button. A dialog box appears and prompts you to choose a file storage location in the network. Scroll to the location in which you want to save the text file, and enter a filename in the appropriate field. Click on the Export button. The results text file is saved in the specified location.

ii Choose File→Close from the View Selected form to close the View Selected form.

14 Click on the OK button or Cancel button to close the CLI Script (Edit) form.

15 Close the Scripts form.

Procedure 32-42 To configure an 802.3ah EFM OAM diagnostic

EFM OAM, which is described in 802.3ah, clause 57, defines the Ethernet OAM sublayer, which provides mechanisms for monitoring link operation, such as remote fault indication and remote loopback control.

The OAM information is transported in slow protocol frames, which are called OAMPDUs. OAMPDUs contain the appropriate control and status information that is used to monitor, test, and troubleshoot OAM-enabled links. OAMPDUs traverse a single link, that is passed between peer OAM entities.

802.3ah EFM OAM supports:

- EFM OAM capability discovery
- active and passive modes
- remote failure indication
- local and remote loopbacks
- EFM OAMPDU tunneling
- high-resolution EFM OAM timers

The 5620 SAM supports EFM OAM diagnostic configuration on Ethernet ports in network mode on the 7210 SAS-E, 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, 7450 ESS, 7705 SAR, 7710 SR, 7750 SR, and 7950 XRS.

For OmniSwitch NEs, see Procedure 32-43.



Caution — Performing an 802.3ah diagnostic is service-affecting. Ensure that you consider the implications of performing this test before you proceed.



Note — In order for the 802.3ah diagnostic to be successful, the local and peer ports must support the 802.3ah protocol, and be operationally and administratively up.

When a port is in loopback mode, service mirroring does not work if the port is a mirror source or a mirror destination.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure an 802.3ah EFM OAM diagnostic and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level and click on a port object. The Physical Port (Edit) form opens with the General tab displayed.

5 Click on the Ethernet tab. The Ethernet port configuration form opens with the General tab displayed.

6 Click on the 802.3ah tab. The 802.3ah form opens.

7 Configure the parameters:

- Administrative State
- Tunneling
- Mode
- Transmit Interval
- Multiplier (Intervals)
- Received Remote Loopback Requests
- Set Remote Loopback
- Set Local Loopback
- Hold Time (s)
- Ignore EFM State
- Grace Tx State Enable

8 Click on the Apply button. A dialog box appears.

9 Click on the Yes button.

10 Click on the Resync button.

11 The 802.3ah form is updated with the results of the 802.3ah diagnostic. The values that are displayed on the form depend on the configuration of the local and peer ports.

Tables 32-3, 32-4, and 32-5 describe the displayed information.

Table 32-3 802.3ah EFM OAM results

Parameter	Value	Description
Operational Status (dot3OamOperStatus)	Disabled	The Administrative State parameter on the local port is set to Disabled.
	Active Send Local	The Mode parameter is set to Active and the local port is discovering the peer port EFM OAM capabilities.
	Passive Wait	The Mode parameter is set to Passive and the local port is waiting to receive OAMPDUs from the peer device.
	Send Local and Remote	The local port discovered the peer but has not yet accepted or rejected the configuration of the peer. The local port may determine that the peer port is not compatible and decline OAM peering.
	OAM Peering Locally Rejected	The local port declined OAM peering.
	Send Local and Remote Ok	The local port accepted OAM peering.
	OAM Peering Remotely Rejected	The remote port declined OAM peering.
	Operational	The local and remote ports accepted the OAM peering.
	Non-operational Half Duplex	The Administrative State parameter is set to Enabled but the local port is in half-duplex mode.
	Link Fault	The link detected a fault and is transmitting OAMPDUs with a link fault indication.

(1 of 2)

Parameter	Value	Description
Max. PDU Size (dot3OamMaxOamPduSize)	PDU size	The largest OAMPDU size, in bytes, that is supported by the local port: Minimum is 64 Maximum is 1518 Default is 1514
Configuration Revision (dot3OamConfigRevision)	0 to 65 535	The configuration revision of the OAM entity obtained from the latest OAMPDU sent by the OAM entity. The value is used by OAM entities to indicate that configuration changes occurred that may require the peer OAM entity to re-evaluate whether OAM peering is allowed.
Functions Supported (dot3OamFunctionsSupported)	Event Support	The port can send and receive event notification OAMPDUs.
	Loopback Support	The port can initiate and respond to loopback commands.
	Unidirectional Support	The port supports the transmission of OAMPDUs on links that operate in unidirectional mode.
	Variable Support	The port can send and receive variable request and response OAMPDUs.
Loopback Status (dot3OamLoopbackStatus)	No Loopback	The port is not in a loopback condition.
	Initiating Loopback	The local device initiated a loopback, sent a loopback OAMPDU and is waiting for a response from the peer port.
	Remote Loopback	The peer port is in loopback mode.
	Terminating Loopback	The local port is in the process of terminating a loopback on the peer port.
	Local Loopback	The peer port has put the local port into loopback mode.
	Unknown	An OAMPDU that contains an unexpected message was received by the local port.

(2 of 2)

Table 32-4 802.3ah EFM OAM Statistics

Statistics	Displayed Value	Description
Frames Lost Due to OAM(dot3OamFramesLostDueToOam)	*Number of frames*	The number of frames that were dropped by the OAM multiplexer. Discontinuities of this counter can occur under some conditions.
Information Rx (dot3OamInformationRx)	*Number of OAMPDUs*	The number of information OAMPDUs received on this interface

(1 of 2)

Statistics	Displayed Value	Description
Information Tx (dot3OamInformation Tx)	*Number of OAMPDUs*	The number of information OAMPDUs transmitted on this interface. Discontinuities of this counter can occur can occur under some conditions.
Loopback Control Rx (dot3OamLoopbackControlRx)	*Number of OAMPDUs*	The number of loopback control OAMPDUs received on this interface
Loopback Control Tx (dot3OamLoopbackConrolTx)	*Number of OAMPDUs*	The number of loopback control OAMPDUs transmitted on this interface
Unsupported Codes Rx (dot3OamUnsupportedCodesRx)	*Number of OAMPDUs*	The number of OAMPDUs received on this interface with an unsupported opcode
Unsupported Codes Tx (dot3OamUnsupportedCodesTx)	*Number of OAMPDUs*	The number of OAMPDUs transmitted on this interface with an unsupported opcode

(2 of 2)

Table 32-5 802.3ah EFM OAM peer information

Peer Information	Displayed Value	Description
Peer MAC Address (dot3OamPeerMacAddress)	*MAC address*	The MAC address of the peer port. The MAC address is contained in the received OAMPDU.
Peer Vendor OUI (dot3OamPeerVendorOui)	*OUI*	The OUI of the OAM peer. The OUI is part of the peer MAC address contained in the received OAMPDU. The OUI can be used to identify the vendor of the remote OAM device.
Peer Vendor Info (dot3OamPeerVendorInfo)	*Vendor information text*	The vendor information field is in the local information TLV, and can be used to determine additional information about the peer device.
Peer Mode (dot3OamPeerMode)	Active or Passive	See Mode
Peer Max PDU Size (dot3OamPeerMaxOamPduSize)	*PDU size*	The largest OAMPDU value, in bytes, that is supported by the peer port. Minimum is 64 Maximum is 1518 Default is 1514
Peer Configuration Revision (dot3OamPeerConfigRevision)	0 to 65 535	The configuration revision of the OAM device as identified in the latest OAMPDU sent by the OAM peer. The configuration revision is used by OAM devices to indicate that configuration changes have occurred which might require the peer OAM device to re-evaluate whether OAM peering is allowed.
Peer Functions Supported (dot3OamPeerFunctSupported)	Event Support	The peer port can send and receive Event Notification OAMPDUs.
	Loopback Support	The peer port can initiate and respond to loopback commands.
	Unidirectional Support	The peer port supports the transmission of OAMPDUs on links that are operating in unidirectional mode.
	Variable Support	The peer port can send and receive Variable Request and Response OAMPDUs.

12 Close the 802.3ah form when you have completed the EFM OAM diagnostic.

Procedure 32-43 To configure an 802.3ah EFM OAM diagnostic on an OmniSwitch at the NE or port level

EFM OAM, which is described in 802.3ah, clause 57, defines the Ethernet OAM sublayer, which provides mechanisms for monitoring link operation, such as remote fault indication and remote loopback control.

The OAM information is transported in slow protocol frames, which are called OAMPDUs. OAMPDUs contain the appropriate control and status information that is used to monitor, test, and troubleshoot OAM-enabled links. OAMPDUs traverse a single link, that is passed between peer OAM entities.

802.3ah EFM OAM supports:

- EFM OAM capability discovery
- active and passive modes
- remote failure indication
- local and remote loopbacks
- high-resolution EFM OAM timers

The EFM OAM diagnostic is supported at the NE level or at the Ethernet port level on the Ethernet ports in network mode.



Caution 1 — Performing an 802.3ah diagnostic is service-affecting. Ensure that you consider the implications of performing this test before you proceed.

Caution 2 — Link OAM (802.3ah) is not supported on mirroring ports.

Caution 3 — When a port is in loopback mode, service mirroring does not work if the port is a mirror source or a mirror destination.



Note — In order for the 802.3ah diagnostic to be successful, the local and peer ports must support the 802.3ah protocol, and be operationally and administratively up.

To configure Link OAM at the NE level, go to Step 1.To configure Link OAM and 802.3ah EFM OAM diagnostics at the port level, go to Step 6.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the OmniSwitch NEs icon.

3 Right-click on the OmniSwitch device where you want to configure an 802.3ah EFM OAM diagnostic and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 Click on the Globals tab.

5 Click on the 802.3ah tab. The 802.3ah form opens.

6 Configure the parameters:

- Administrative Status
- Multiple PDU Count
- Statistics
- Log-history

7 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

8 Expand to the port level and click on a port object. The Physical Port (Edit) form opens with the General tab displayed.

9 Click on the Ethernet tab. The Ethernet port configuration form opens with the General tab displayed.

10 Click on the 802.3ah tab. The 802.3ah form opens.

11 Configure the parameters:

- Administrative State
- Mode
- Transmit Interval
- Received Remote Loopback Requests
- Set Local Loopback
- Set Local Loopback
- Hold Time (s)
- Dying Gasp Notify
- Critical Event Notify
- Statistics
- Log-history
- Errored Frame Window (dsec)
- Errored Frame Period Window (frames)
- Errored Frame Seconds Summary Window (dsec)
- Threshold (frames)
- Period Threshold (frames)
- Seconds Summary Threshold (framesec)
- Notify
- Period Notify
- Seconds Summary Notify
- Number of Frames
- Frames Delay (ms)
- Start L1-Ping

12 Click on the Apply button. A dialog box appears.

13 Click on the Yes button.

14 The 802.3ah form is updated with the results of the 802.3ah diagnostic. The values that are displayed on the form depend on the configuration of the local and peer ports.

Tables 32-6, 32-7, and 32-8 describe the displayed information.

Table 32-6 802.3ah EFM OAM results

Parameter	Value	Description
Operational Status (dot3OamOperStatus)	Disabled	The Administrative State parameter on the local port is set to Disabled.
	Active Send Local	The Mode parameter is set to Active and the local port is discovering the peer port EFM OAM capabilities.
	Passive Wait	The Mode parameter is set to Passive and the local port is waiting to receive OAMPDUs from the peer device.
	Send Local and Remote	The local port discovered the peer but has not yet accepted or rejected the configuration of the peer. The local port may determine that the peer port is not compatible and decline OAM peering.
	OAM Peering Locally Rejected	The local port declined OAM peering.
	Send Local and Remote Ok	The local port accepted OAM peering.
	OAM Peering Remotely Rejected	The remote port declined OAM peering.
	Operational	The local and remote ports accepted the OAM peering.
	Non-operational Half Duplex	The Administrative State parameter is set to Enabled but the local port is in half-duplex mode.
	Link Fault	The link detected a fault and is transmitting OAMPDUs with a link fault indication.
Max. PDU Size (dot3OamMaxOamPduSize)	PDU size	The largest OAMPDU size, in bytes, that is supported by the local port: Minimum is 64 Maximum is 1518 Default is 1514
Configuration Revision (dot3OamConfigRevision)	0 to 65 535	The configuration revision of the OAM entity obtained from the latest OAMPDU sent by the OAM entity. The value is used by OAM entities to indicate that configuration changes occurred that may require the peer OAM entity to re-evaluate whether OAM peering is allowed.
Functions Supported (dot3OamFunctionsSupported)	Event Support	The port can send and receive event notification OAMPDUs.
	Loopback Support	The port can initiate and respond to loopback commands.
	Unidirectional Support	The port supports the transmission of OAMPDUs on links that operate in unidirectional mode.
	Variable Support	The port can send and receive variable request and response OAMPDUs.

(1 of 2)

Parameter	Value	Description
Loopback Status (dot3OamLoopbackStatus)	No Loopback	The port is not in a loopback condition.
	Initiating Loopback	The local device initiated a loopback, sent a loopback OAMPDU and is waiting for a response from the peer port.
	Remote Loopback	The peer port is in loopback mode.
	Terminating Loopback	The local port is in the process of terminating a loopback on the peer port.
	Local Loopback	The peer port has put the local port into loopback mode.
	Unknown	An OAMPDU that contains an unexpected message was received by the local port.

(2 of 2)

Table 32-7 802.3ah EFM OAM Statistics

Statistics	Displayed Value	Description
Frames Lost Due to OAM(dot3OamFramesLostDueToOam)	*Number of frames*	The number of frames that were dropped by the OAM multiplexer. Discontinuities of this counter can occur under some conditions.
Information Rx (dot3OamInformationRx)	*Number of OAMPDUs*	The number of information OAMPDUs received on this interface
Information Tx (dot3OamInformation Tx)	*Number of OAMPDUs*	The number of information OAMPDUs transmitted on this interface. Discontinuities of this counter can occur can occur under some conditions.
Loopback Control Rx (dot3OamLoopbackControlRx)	*Number of OAMPDUs*	The number of loopback control OAMPDUs received on this interface
Loopback Control Tx (dot3OamLoopbackConrolTx)	*Number of OAMPDUs*	The number of loopback control OAMPDUs transmitted on this interface
Unsupported Codes Rx (dot3OamUnsupportedCodesRx)	*Number of OAMPDUs*	The number of OAMPDUs received on this interface with an unsupported opcode
Unsupported Codes Tx (dot3OamUnsupportedCodesTx)	*Number of OAMPDUs*	The number of OAMPDUs transmitted on this interface with an unsupported opcode

Table 32-8 802.3ah EFM OAM peer information

Peer Information	Displayed Value	Description
Peer MAC Address (dot3OamPeerMacAddress)	*MAC address*	The MAC address of the peer port. The MAC address is contained in the received OAMPDU.
Peer Vendor OUI (dot3OamPeerVendorOui)	*OUI*	The OUI of the OAM peer. The OUI is part of the peer MAC address contained in the received OAMPDU. The OUI can be used to identify the vendor of the remote OAM device.
Peer Vendor Info (dot3OamPeerVendorInfo)	*Vendor information text*	The vendor information field is in the local information TLV, and can be used to determine additional information about the peer device.
Peer Mode (dot3OamPeerMode)	Active or Passive	See Mode
Peer Max PDU Size (dot3OamPeerMaxOamPduSize)	*PDU size*	The largest OAMPDU value, in bytes, that is supported by the peer port. Minimum is 64 Maximum is 1518 Default is 1514
Peer Configuration Revision (dot3OamPeerConfigRevision)	0 to 65 535	The configuration revision of the OAM device as identified in the latest OAMPDU sent by the OAM peer. The configuration revision is used by OAM devices to indicate that configuration changes have occurred which might require the peer OAM device to re-evaluate whether OAM peering is allowed.
Peer Functions Supported (dot3OamPeerFunctSupported)	Event Support	The peer port can send and receive Event Notification OAMPDUs.
	Loopback Support	The peer port can initiate and respond to loopback commands.
	Unidirectional Support	The peer port supports the transmission of OAMPDUs on links that are operating in unidirectional mode.
	Variable Support	The peer port can send and receive Variable Request and Response OAMPDUs.

15 Close the 802.3ah form when you have completed the EFM OAM diagnostic.

Procedure 32-44 To view OAM diagnostic test results

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose Test Result (Assurance) from the object drop-down list.

All test result types are listed under the Test Result (Assurance) item. Expand the Ping Result (Assurance) and Trace Result (Assurance) objects to display the test result types for ping- and trace-related tests.

3 Select a filter option. Use the configurable filters choices and properties options on the Service Test Manager form and click on the Search button. The list of test results that meet the filter criteria are displayed.

4 Choose a test result from the list and click on the Properties button. The appropriate OAM diagnostic test results form opens with the General tab displayed.

5 Click on the form tabs to view the test results for the OAM diagnostic. You can click on the View button beside an object and open the properties form for the object.

a CFM Continuity Check OAM diagnostic information includes:

- identifies the MD and MEG involved in the test
- MEP creation on a SAP
- MEP creation on a SDP
- intervals (seconds) between continuity checks
- MHF creation

b CFM loopback OAM diagnostic information includes:

- originating NE
- originating MEP
- destination MAC addresses
- data size
- VLAN priority
- number of messages sent

c CFM link trace OAM diagnostic information includes:

- originating NE
- originating MEP
- target MAC addresses
- TTL

d CFM One Way OAM diagnostic information includes:

- originating NE
- originating MEP
- destination MAC addresses
- priority

e CFM Two Way OAM diagnostic information includes:

- originating NE
- originating MEP
- destination MAC addresses
- VLAN priority

f CFM Single Ended Loss OAM diagnostic information includes:

- originating NE
- originating MEP
- destination MAC addresses
- test duration, in seconds
- number of LMR frames received
- number of frames transmitted by the far end
- number of frames received by the near end
- number of frames lost at the near end
- percentage of frames lost at the near end
- number of frames transmitted by the near end
- number of frames received by the far end
- number of frames lost at the far end
- percentage of frames lost at the far end

g CFM Eth Test OAM diagnostic information includes:

- originating NE
- originating MEP
- destination MAC addresses
- data size
- VLAN priority

h CFM Two Way SLM diagnostic information includes:

- Global Maintenance Entity Group
- Originating MEP

i MTU ping OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- source and destination site IP addresses
- originating tunnel ID
- administrative and operational states
- information about previous diagnostics, including the start and finish sizes of the MTU datagram (packet)
- ID of the service being diagnosed
- name of the service being diagnosed
- MTU response size, indicating the largest packet size that the tunnel can transport

j Tunnel ping OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- source and destination site IP addresses
- originating and return tunnel IDs
- administrative state
- operational state
- probes to be issued information
- message size
- forwarding class used by the service
- ID of the service being diagnosed
- name of the service being diagnosed
- average, minimum, and maximum one-way time values, in microseconds, with a value of 0 indicating that no one-way trip measurement is available
- sum-of-squares one-way time for all ping responses received, used to enable a standard deviation calculation
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available

k VPRN ping diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source IP addresses
- service ID and name
- number of probes to be issued
- operational size
- number of responses
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available
- inner and outer encapsulation value of the SAP supporting the requested ping response, when the address type is a SAP and in the case that the inner encapsulation value is from a 5620 SAM-managed device

l VPRN trace diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source IP addresses
- service ID and name
- number of probes to be issued
- operational size
- number of responses

m VPRN ICMP ping diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source IP addresses
- operational size
- number of responses
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available

n VPRN ICMP trace diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target IP addresses
- operational size
- number of responses
- initial and maximum time to live
- time to wait (microseconds)

o MAC ping diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source MAC addresses
- service ID and name
- number of probes to be issued
- administrative and operational states
- information about previous diagnostics
- average, minimum, and maximum round-trip time values, in microseconds, with a value of 0 indicating no round-trip measurement is available
- sum-of-squares round-trip time for all ping responses received, used to enable a standard deviation calculation

p MAC trace diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source MAC addresses
- service ID and name
- number of probes to be issued
- administrative and operational states
- information about previous diagnostics

q Service site ping OAM diagnostic information includes:

- target and source IP addresses
- service ID and name
- probes to be issued information
- check mark buttons to specify whether a local tunnel, remote tunnel, or local and remote tunnel is performed
- information about previous service site OAM diagnostics, including probes sent and responses received, loss percentage, packet timeouts, and last good packet time
- ID of the service being diagnosed

r VCCV ping OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- IP address of the destination and far-end devices
- time of last response
- number of responses received
- response time
- loss indicator, with a value of 0 indicating that the test packet was received and a value of 1 indicating that the test packet was lost
- sum-of-squares one-way trip time for all ping responses received, used to enable a standard deviation calculation

s VCCV trace OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- number of probes to be issued
- time of last response
- source and response IP addresses
- number of hops
- probe responses from NEs in path

t LSP ping diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source IP addresses
- service ID and name
- number of probes to be issued
- operational size
- number of responses
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available
- average, minimum, and maximum one-way trip time values, in microseconds, with a value of 0 indicating that no one-way trip measurement is available
- sum-of-squares one-way trip time for all ping responses received, used to enable a standard deviation calculation

u P2MP LSP ping diagnostic information includes:

- information about the configuration test, including the configured parameter values
- test probe: size, Time to Live, Forwarding Class, Forwarding Profile
- results: probes sent, responses received, probe timeouts, probes lost
- probe result status
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available
- average, minimum, and maximum outbound and inbound one-way trip time values, in microseconds, with a value of 0 indicating that no one-way trip measurement is available
- sum-of-squares one-way trip time for all ping responses received, used to enable a standard deviation calculation

v P2MP LSP trace diagnostic information includes:

- information about the configuration test, including the configured parameter values
- trace attempt: size, Initial Time to Live, Forwarding Class, Forwarding Profile
- probe result status
- number of probes sent
- responses received
- timeouts
- failures
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available
- average, minimum, and maximum outbound and inbound one-way trip time values, in microseconds, with a value of 0 indicating that no one-way trip measurement is available
- sum-of-squares one-way trip time for all ping responses received, used to enable a standard deviation calculation

w LDP Tree Trace Result diagnostic information includes:

- information about the configuration test, including the configured parameter values
- number and IP address of hops included in the test
- destination IP address of the path associated with the hop
- next hop IP address
- a display of available hops in a tree format

x Multicast router OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source IP addresses
- status of diagnostic
- number of sent, received, and lost packets
- packet loss percentage
- number of packet timeouts
- time for last successful contact with the target IP address

y Multicast trace OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- source and group multicast addresses
- destination and response IP addresses
- virtual router ID
- number of hops in path
- response from NEs in path
- number of trace attempts
- number of successful traces
- time for last successful trace
- identifier if multicast path changed from last successful trace

z Multicast FIB ping OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source IP addresses
- service ID and name
- number of probes to be issued
- operational size
- number of responses
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available
- average, minimum, and maximum one-way trip time values, in microseconds, with a value of 0 indicating that no one-way trip measurement is available
- sum-of-squares one-way trip time for all ping responses received, used to enable a standard deviation calculation

aa ICMP ping OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source IP addresses
- virtual router ID
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available
- average, minimum, and maximum round-trip time values, in microseconds, with a value of 0 indicating that no round-trip measurement is available
- sum-of-squares one-way trip time for all ping responses received, used to enable a standard deviation calculation

ab ICMP trace OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- source and target IP addresses
- virtual router ID
- number of hops
- probe responses from managed devices
- number of trace probe attempts
- number of successful traces
- time for last successful trace
- initial and maximum time to live values

ac CPE ping OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- destination and source IP addresses
- source MAC address (VPLS only)
- average, minimum, and maximum round-trip time values, in microseconds, with a value of 0 indicating that no round-trip measurement is available
- sum-of-squares one-way trip time for all ping responses received, used to enable a standard deviation calculation
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available

ad DNS ping OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- average, minimum, and maximum round-trip time values, in microseconds, with a value of 0 indicating that no round-trip measurement is available
- sum-of-squares round-trip time for all ping responses received, used to enable a standard deviation calculation
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available
- the IP Address for the requested DNS name, as reachable by the DNS server, shown for IPv4 addresses in dotted-decimal format
- status, including response received to indicate a successfully completed diagnostic

ae ANCP ping OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- source and destination site IP addresses
- administrative and operational states
- ID of the circuit being diagnosed
- information about previous ANCP OAM diagnostics, including packet history size, probes sent and responses received, and packet failure

Procedure 32-45 To interpret OAM diagnostic results

1 Perform the OAM diagnostic, as described in Procedure 32-1 to Procedure 32-33.

2 Perform Procedure 32-44 to view OAM diagnostic test results.

3 The General and Response Packets tabs display the key information about OAM diagnostic results.

When there no packet information is required, as for an OAM ping, the information appears on the Packets Results form without any tabs.

For example, status and return code information appears directly on the Packets Results form.

You can view test packet information by performing the following actions:

i Click on the Response Packets tab. A list of test objects appears.

ii Choose an object from the display and click on the Properties button. The Packets Results form opens.

4 Interpret the results, based on the status and return code information.

a For MTU OAM diagnostics, the key information is how many frames were sent and incrementally increased in size before the frames could not be sent.

When the frame cannot be sent because it is too large, that results in a request timeout message. The largest frame that was sent is the last frame size with an associated success response.

b For tunnel OAM diagnostics, the key information is the result of the diagnostic, displayed in the status message. Table 32-9 lists the displayed messages and descriptions.

Table 32-9 Tunnel OAM diagnostics results

Displayed message	Description
Request Timeout	The request timed out with a reply.
Orig-SDP Non-Existent	The request was not sent because the originating SDP does not exist.
Orig-SDP Admin-Down	The request was not sent because the originating SDP administrative state is operationally down.
Orig-SDP Oper-Down	The request was not sent because the originating SDP operational state is down.
Request Terminated	The operator terminated the request before a reply could be received or before the timeout of the request could occur.
Far End: Originator-ID Invalid	The request was received by the far end, but the far end indicates that the originating SDP ID is invalid.
Far End: Responder-ID Invalid	The request was received by the far end, but the responder ID is not the same destination SDP ID that was specified.
Far End:Resp-SDP Non-Existent	The reply was received, but the return SDP ID used to respond to the request does not exist
Far End:Resp-SDP Invalid	The reply was received, but the return SDP ID used to respond to the request is invalid.
Far End:Resp-SDP Down	The reply was received, but the return SDP ID indicates that the administrative or operational state of the SDP is down.
Success	The tunnel is in service and working as expected. A reply was received without any errors.

c For service site OAM diagnostics, the key information is the result of the diagnostic, which is displayed in the status message and with the other records from the General tab.

As the diagnostic traverses the service across the originating and destination IP addresses, the service tunnels, and the used VCs, the status of each portion of the service is displayed. Table 32-10 lists the displayed messages and descriptions.

Table 32-10 Service site OAM diagnostics results

Displayed message	Description
Sent - Request Timeout	The request timed out with a reply.
Sent - Request Terminated	The request was not sent because the diagnostic was terminated by the operator.
Sent - Reply Received	The request was sent and a successful reply message was received.
Not Sent - Non-Existent Service-ID	The configured service ID does not exist.
Not Sent - Non-Existent SDP for Service	There is no SDP for the service being tested.
Not Sent - SDP For Service Down	The SDP for the service is down.
Not Sent - Non-Existent Service Egress Label	There is a service label mismatch between the originator and responder.

d For MAC, VPRN, and multicast FIB ping OAM diagnostics, the key information is the result of the diagnostic. Table 32-11 lists the displayed messages, the return code, and descriptions.

Table 32-11 MAC, VPRN, multicast FIB ping OAM diagnostics results

Displayed message (return code)	Description
notApplicable (0)	The OAM diagnostic message does not apply to the OAM diagnostic performed.
fecEgress (1)	The replying router is an egress for the FEC.
fecNoMap (2)	The replying router has no mapping for the FEC.
notDownstream (3)	The replying router is not a downstream router.
downstream (4)	The replying router is a downstream router, and the mapping for this FEC on the router interface is the specified label.
downstreamNotLabel (5)	The replying router is a downstream router, and the mapping for this FEC on the router interface is not the specified label.
downstreamNotMac (6)	The replying router is a downstream router, but it does not have the specified MAC address.
downstreamNotMacFlood (7)	The replying router is a downstream router, but it does not have the specified MAC address and cannot flood the request to other routers.
malformedEchoRequest (8)	The received echo request is malformed.
tlvNotUnderstood (9)	One or more TLVs were not understood.
downstreamNotInMFib (10)	The replaying router is a downstream router, but it is not part of the MFIB.

(1 of 2)

Displayed message (return code)	Description
Downstream mapping mismatched (11)	The downstream mapping is mismatched.
Upstream interface index unknown (12)	The upstream interface index is unknown.
Label switched but no MPLS forwarding at stack-depth (13)	The label switched successfully but MPLS forwarding did not occur at stack-depth.
No label entry at stack-depth (14)	The label entry at stack-depth did not occur.
Protocol not associated with interface at FEC stack-depth (15)	The protocol is not associated with the interface at FEC stack-depth.
Premature termination of ping due to label stack shrinking to a single label (16)	The ping was terminated prematurely due to the label stack shrinking to a single label.

(2 of 2)

e For multicast router OAM diagnostics, the key information includes information that is related to adjacent routers, supported protocols, traffic metrics, and time-to-live thresholds. Administrators can use this information to identify bidirectional adjacency relationships.

f For multicast trace OAM diagnostics, the key information is the result of the diagnostic, displayed in the status message. Table 32-12 lists the displayed messages and descriptions.

Table 32-12 Multicast trace OAM diagnostics results

Displayed message	Description
No Error	No error.
Wrong Interface	The router not forwarding the multicast source or group traffic because the router is not part of the multicast path.
Prune Sent	The router sent a prune request upstream that impacts the multicast source and group in the trace request.
Prune Received	The router stopped forwarding traffic for the multicast source and group in response to a request from the next hop router.
Scoped	The multicast group is subject to administrative scoping.
No Route	The router has no route for the multicast source or group and no way to determine a potential route.
Wrong Last Hop	The router is not the correct last-hop router.
Not Forwarding	The router is not forwarding the multicast source or group traffic for an unspecified reason.
Reached RP or Core	Request arrived on the rendezvous point or core.
Request on RPF	The request arrived on the expected RPF interface.
No Multicast	The request arrived on an interface that is not enabled for multicast traffic.
Hops Hidden	One or more hops are hidden from the trace.
Fatal Error	Fatal error.
No Space	There is insufficient room to insert another response data block in the packet.
Old Router	The previous router hop cannot process the multicast trace request.
Admin. Prohibited	The multicast trace was administratively prohibited.
Unknown	—

g For most diagnostics, some common return codes are used. The return codes indicate the status of OAM tests, usually when there was a problem performing the test. Table 32-13 lists the messages, return codes, and descriptions.

Table 32-13 OAM diagnostics return codes

Displayed message (return code)	Description
responseReceived (1)	A response was received on the device to the OAM diagnostic performed.
unknown (2)	The OAM diagnostic failed for an unknown reason.
internalError (3)	An internal error on the device caused the diagnostic to not be performed.
maxConcurrentLimit Reached (4)	The device cannot perform the OAM diagnostics because there are too many OAM diagnostic operations already running.
requestTimedOut (5)	The OAM diagnostic could not be completed because no reply was received within the allocated timeout period.
unknownSDPOrigin (6)	Indicates an invalid or non-existent originating service tunnel.
downOrigSdpId (7)	The originating service tunnel is operationally down.
requestTerminated (8)	The OAM diagnostic was cancelled before the timeout or reply period was reached.
invalidOriginatorId (9)	The far-end device replied indicating that the originating ID was invalid.
invalidResponderId (10)	The far-end device replied with an invalid responding ID.
unknownRespSdpId (11)	The far-end device replied with an invalid response service tunnel ID.
downRespSdpId (12)	The responding service tunnel with the given ID is operationally or administratively down.
invalidServiceId (13)	An invalid or non-existent service ID.
invalidSdp (14)	An invalid or non-existent service tunnel for the service.
downServiceSdp (15)	The service tunnel bound to the service is down.
noServiceEgressLabel (16)	The egress label for the service does not exist.
invalidHostAddress (17)	The IP address for the host is invalid, for example, in the case of a broadcast or multicast IP address.
invalidMacAddress (18)	The MAC address specified in the OAM diagnostic is invalid.
invalidLspName (19)	The LSP name specified in the OAM diagnostic is invalid.
macIsLocal (20)	The MAC address is the local SAP or device MAC address, not the MAC address of the downstream SAP or device, therefore the MAC ping or trace cannot be sent.
farEndUnreachable (21)	No route is available to the far-end GRE service tunnel.
downOriginatorId (22)	The originating ping device is operationally down.
downResponderId (23)	The device responding to the ping is operationally down.
changedResponderId (24)	The ID of the device responding to the ping has changed.
downOrigSvcId (25)	The originating service identified by the ID is operationally down.
downRespSvcId (26)	The service responding to the ping identified by the ID is operationally down.
noServiceIngressLabel (27)	The ingress label for the service does not exist.
mismatchCustId (28)	The subscriber ID identified with the service differs from the originating device compared to the responding device.
mismatchSvcType (29)	The service type identified with the service differs from one device to another.
mismatchSvcMtu (30)	The service MTU size associated with the service differs from the originating device compared to the responding device.
mismatchSvcLabel (31)	The service label identified with the service differs from the originating device compared to the responding device.

(1 of 4)

Displayed message (return code)	Description
noSdpBoundToSvc (32)	There is no service tunnel bound to the service.
downOrigSdpBinding (33)	The service tunnel associated with the originating device's service is operationally down.
invalidLspPathName (34)	The LSP path name specified in the OAM diagnostic is invalid.
noLspEndpointAddr (35)	There is no LSP endpoint address specified in the OAM diagnostic.
noActiveLspPath (36)	There is no active LSP path.
downLspPath (37)	The far end of the LSP is operationally down.
invalidLspProtocol (38)	The LSP protocol is not valid or is not supported.
invalidLspLabel (39)	The LSP label is invalid.
routeIsLocal (40)	For a VPRN ping, the route is a local route.
noRouteToDest (41)	For a VPRN ping, there is no route available to the destination of the OAM diagnostic.
localExtranetRoute (42)	For a VPRN ping, the route is a local extranet route.
srcIpInBgpVpnRoute (43)	For a VPRN ping, the source IP address belongs to a BGP VPN route.
srcIpInvalid (44)	For a VPRN ping, the source IP address is invalid or no route is available to the source IP address.
bgpDaemonBusy (45)	For a VPRN trace, the BGP routing process is busy on the device, and VPRN route target information cannot be retrieved.
mcastNotEnabled (46)	Multicast is not enabled on the device, so the diagnostic cannot be performed.
mTraceNoSGFlow (47)	—
mTraceSysIpNotCfg (48)	The system IP address is not configured. The address is required for a response to a multicast trace.
noFwdEntryInMfib (49)	No forwarding entry could be found for the specified source and destination addresses in the MFIB.
dnsNameNotFound (50)	The domain name specified in the dns query does not exist
noSocket (51)	For icmp-ping, unable to get socket.
socketOptVprnIdFail (52)	For icmp-ping, unable to set SO_VPRNID for socket.
socketOptIfInexFail (53)	For icmp-ping, unable to set IP_IFINDEX for socket.
socketOptNextHopFail (54)	For icmp-ping, unable to set IP_NEXT_HOP for socket.
socketOptMtuDiscFail (55)	For icmp-ping, unable to set IP_MTU_DISC for socket.
socketOptSndbufFail (56)	For icmp-ping, unable to set SO_SNDBUF for socket.
socketOptHdrincFail (57)	For icmp-ping, unable to set IP_HDRINCL for socket.
socketOptTosFail (58)	For icmp-ping, unable to set IP_TOS for socket.
socketOptTtlFail (59)	For icmp-ping, unable to set IP_TTL for socket.
bindSocketFail (60)	For icmp-ping, unable to bind socket.
noRouteByIntf (61)	For icmp-ping, no route to destination via the specified interface.
noIntf (62)	For icmp-ping, no interface specified.
noLocalIp (63)	For icmp-ping, unable to find local ip address.
sendtoFail (64)	For icmp-ping, sendto function failed.

(2 of 4)

Displayed message (return code)	Description
rcvdWrongType (65)	For icmp-ping, received packet of wrong icmp type.
noDirectInterface (66)	For icmp-ping, no direct interface to reach destination.
nexthopUnreachable (67)	For icmp-ping, unable to reach the next-hop.
socketOptHwTimeStampFail (68)	For icmp-ping, unable to set IP_TIM_TIME for socket.
noSpokeSdpInVll (69)	For vccv-ping, unable to find spoke-sdp given SdpId:vc-id
farEndVccvNotSupported (70)	For vccv-ping, far end does not support the VCCV options.
noVcEgressLabel (71)	For vccv-ping, no Vc egress label to send vccv-ping
socketOptIpSessionFail (72)	For icmp-ping, unable to set IP_SESSION for socket.
rcvdWrongSize (73)	For icmp-ping, received packet of wrong size.
dnsLookupFail (74)	For icmp-ping, dns lookup failed.
noIpv6SrcAddrOnIntf (75)	For icmp-ping, no ipv6 source on the interface.
multipathNotSupported (76)	For lsp-trace, downstream NE does not support multipath.
nhIntfNameNotFound (77)	For lsp-ping/trace, Given next-hop interface name not found.
msPwInvalidReplyMode (78)	For vccv-ping, MS-PW switching NE supports ip-routed reply mode only.
ancpNoAncpString (79)	ANCP string unknown to the system.
ancpNoSubscriber (80)	Subscriber unknown to the system.
ancpNoAncpStringForSubscriber (81)	Subscriber has no associated ANCP string.
ancpNoAccessNodeforAncpString (82)	No access NE is found for the given ANCP string.
ancpNoAncpCapabilityNegotiated (83)	ANCP capability not negotiated with the involved DSLAM.
ancpOtherTestInProgress (84)	Another ANCP test is running for this ANCP string.
ancpMaxNbrAncpTestsInProgress (85)	Maximum number of concurrent ANCP tests reached.
spokeSdpOperDown (86)	For vccv-ping, spoke-sdp is operationally down.
noMsPwVccvInReplyDir (87)	Switching NE in MS-PW with no vccv support in echo reply direction.
p2mpLspNameOrInstInvalid (88)	P2MP LSP name or instance provided is not valid.
p2mpLspS2LPathDown (89)	LSP path to S2L is down.
p2mpLspS2LAddressInvalid (90)	One or more S2L address is not valid.
p2mpLspNotOperational (91)	P2MP LSP is operationally down.
p2mpLspTrMultipleReplies (92)	Probe returned multiple responses. Result may be inconsistent.
invalidMepId (93)	The user-configured MEP identifier is not valid.
multipleReplies (94)	More than one reply received, when one was expected.
packetSizeTooBig (95)	Packet size is too big.
gtpPingError (96)	General GTP Ping Error.
gtpPingRsrcUnavailable (97)	GTP Path management resource unavailable.
gtpPingDupRequest (98)	Duplicate request for the same peer.

(3 of 4)

Displayed message (return code)	Description
gtpPingCleanUpInProg (99)	GTP Path management clean up in progress.
invalidInterface (100)	The egress interface specified does not exist.

(4 of 4)

Procedure 32-46 To configure threshold-crossing alarms on NE-schedulable OAM tests

You can configure threshold-crossing alarms for OAM tests that are NE-schedulable. An alarm is raised when a threshold is crossed, either because the value rose above or fell below the configured level.

You can also configure threshold-crossing alarms on test definitions within a test policy. See Procedure 77-2 for additional information.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Test (Assurance) icon from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of tests is displayed.

5 Choose an NE-schedulable test from the list and click on the Properties button. The Test (Edit) form opens with the General tab displayed.

6 Click on the Threshold Alarms tab.

7 Click on the Create button. The NE Threshold Event (Create) form opens with the General tab displayed.

8 Configure the parameters:

- Type
- Generate Alarm on Rising Threshold
- Clear Alarm on Falling Threshold
- Update Test Result Status
- Include Falling Threshold

9 Click on the Rising Threshold tab.

10 Configure the Threshold Value parameter.

11 Click on the Falling Threshold tab.



Note — The Falling Threshold tab can be accessed only when the Include Falling Threshold parameter is enabled on the General tab of the NM Threshold Event (Create) form.

12 Configure the Threshold Value parameter.

13 Click on the OK button. The NE Threshold Event (Create) form closes.

14 Repeat steps 7 to 13 to configure threshold events on additional tests.

15 Select a test from the list and click on the Execute button. A threshold-crossing alarm appears on the dynamic alarm list if the threshold rises above or falls below the configured level.

16 Close the Test (Edit) form. The Service Test Manager form reappears.

17 Close the Service Test Manager form.

Procedure 32-47 To configure NM threshold-crossing alarms on non-NE-schedulable OAM tests

You can configure NM threshold-crossing alarms for OAM tests that are non-NE-schedulable. NM threshold-crossing alarms are not configurable for service site ping, VPRN trace, MTU ping, Mrinfo and Mtrace tests. An alarm is raised when an NM threshold is crossed, either because the value rose above or fell below the configured level. The type of NM threshold-crossing event available for selection depends on the test type.

You can also configure NM threshold-crossing alarms on test definitions within a test policy. See Procedure 77-3 for additional information.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Test (Assurance) icon from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of tests is displayed.

5 Choose a non-NE-schedulable test from the list and click on the Properties button. The Test (Edit) form opens with the General tab displayed.

6 Click on the NM Threshold Alarms tab.

7 Click on the Create button. The NM Threshold Event (Create) form opens with the General tab displayed.

8 Configure the parameters.

- Type
- Generate Alarm on Rising Threshold
- Clear Alarm on Falling Threshold
- Update Test Result Status
- Include Falling Threshold

9 Click on the NM Rising Threshold tab.

10 Configure the Threshold Value parameter.

11 Click on the NM Falling Threshold tab.



Note — The NM Falling Threshold tab can be accessed only when the Include Falling Threshold parameter is enabled on the General tab of the NM Threshold Event (Create) form.

12 Configure the Threshold Value parameter.

13 Click on the OK button. The NM Threshold Event (Create) form closes, and a dialog box appears.

14 Click on the OK button.

15 Click on the Apply button on the Test (Edit) form. A dialog box appears.

16 Confirm the action. The test appears on the list.

17 Repeat steps 7 to 16 to configure NM threshold events on additional tests.

18 Select a test from the list and click on the Execute button. A threshold-crossing alarm appears on the dynamic alarm list if the threshold rises above or falls below the configured level.

19 Close the Test (Edit) form. The Service Test Manager form reappears.

20 Close the Service Test Manager form.

Procedure 32-48 To edit an OAM diagnostic test

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Test (Assurance) icon from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of tests is displayed.

5 Choose one or more OAM diagnostic tests from the results list and click on the Properties button. The appropriate edit form opens.

6 Change any configurable parameter for the test.

7 Click on the OK button to save the changes. A dialog box appears.

8 Confirm the action. The modified test or tests are shown in the list.

Procedure 32-49 To delete an OAM diagnostic test

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose Test (Assurance) icon from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of tests is displayed.

5 Choose one or more OAM diagnostic tests from the results list and click on the Properties button. The appropriate edit form opens.

6 Choose one or more OAM diagnostic tests from the results list and click on the Delete button. A dialog box appears.

7 Confirm the action. The test or tests are deleted from the list of available OAM diagnostic tests.

Procedure 32-50 To set STM managed device test limits

You can configure the maximum number of pings and traces allowed to be performed from the 5620 SAM by the managed devices, or you can limit the number of tests performed. The default is to allow an unlimited number of tests.



Note 1 — You must enable debug STM mode before you perform this procedure. See Procedure 3-19 for more information.

Note 2 — Limiting the number of tests does not raise an alarm on 5620 SAM or an SNMP trap on the managed device. The indication that the limit has been reached is no returned test results.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose NE Test Agent (Assurance) from the object drop-down list.

3 Click on the Search button. A list of NE Test Agent policies appears, one for each managed device.

4 Choose on one or more policies from the list and click on the Properties button. The configuration form opens.

5 You can set the number of tests allowed for individual managed devices, or for all managed devices, using the following parameters:

- Unlimited Concurrent Pings
- Unlimited Concurrent Traces
- Maximum Concurrent Pings
- Maximum Concurrent Traces

6 Click on the Apply button to save the changes. A dialog box appears.

7 Click on the Yes button to confirm the action.

33 — VRRP

33.1 VRRP overview *33-2*

33.2 Workflow to configure VRRP *33-5*

33.3 VRRP management procedures *33-6*

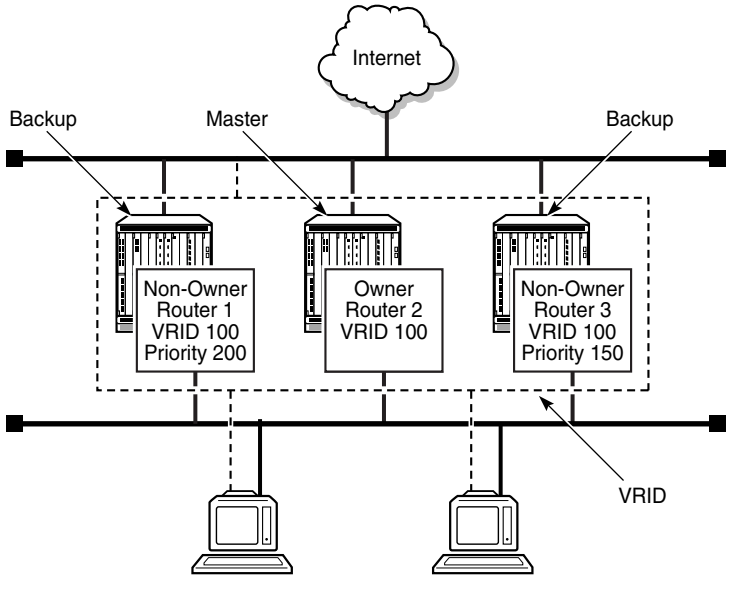
33.1 VRRP overview

The 5620 SAM supports VRRP management. VRRP creates a redundant routing system that takes over packet transmission on a common LAN segment when a router fails. VRRP designates alternative routing paths in the form of virtual routers, or VRs, without changing the IP or MAC address of a protected router.

A VRRP protected router owns the IP address of the VR. The VRRP owner forwards packets using the default gateway. When the owner router fails, packet-forwarding responsibilities are transferred to a designated backup router. This router becomes the master and forwards packets using the VR IP address.

Figure 33-1 shows a basic VR that acts in parallel with the real network. Router 2 is the owner with the address from which packets are forwarded. If Router 2 fails, Router 3, which has been configured to route using the master address in a backup role, begins to forward packets using this IP address. Router 1 is also a backup router, but because its priority number is higher, it ranks below Router 3.

Figure 33-1 VR concepts

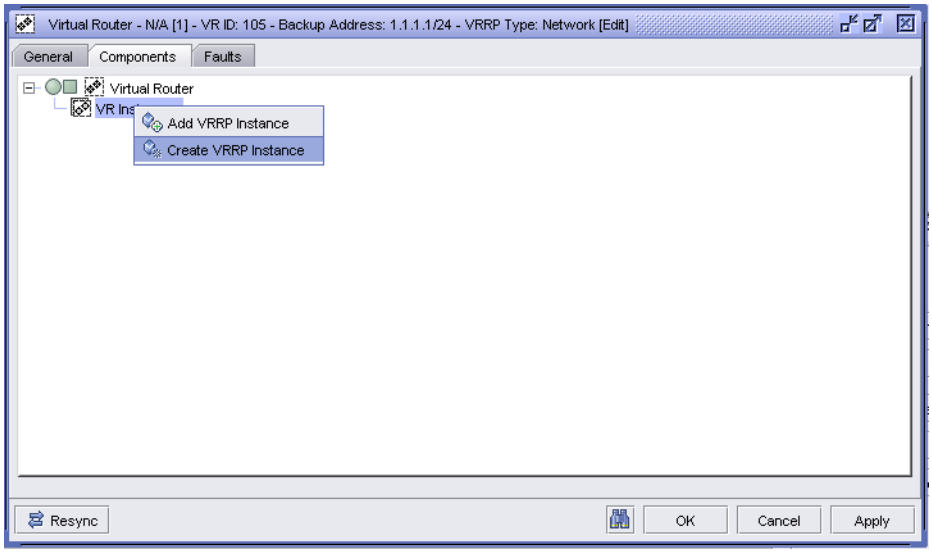


The 5620 SAM supports the configuration of VRs for network interfaces and for L3 access interfaces.

VRRP in an IES involves interfaces from separate IESs. VRRP in a VPRN requires interfaces that are in the same VPRN service. The 5620 SAM supports on-demand, but not scheduled, statistics collection for VRRP in a VPRN. Certain VRRP SNMP traps do not apply to VPRN; see the appropriate NE documentation for information.

You can configure the VR through another set of tabbed forms and a navigation tree, which allows you to add VRRP instances IP owner and non-owner router interfaces, as shown in Figure 33-2.

Figure 33-2 Adding or creating a VRRP instance

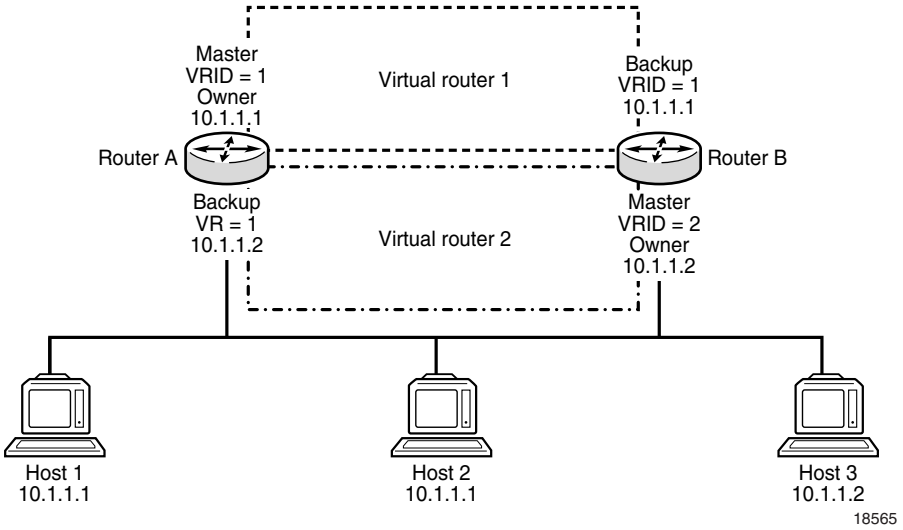


VR

A VR is a logical entity, managed by VRRP, that acts as a default router for hosts on a shared LAN. The VR consists of a VRID and a subnet (that is, ip_address/mask). A VRRP router can back up one or more VRs. The purpose of supporting multiple IP addresses in a single VR is for multi-netting. This common mechanism allows multiple local subnet attachments on a single routing interface. Up to four VRs are allowed on a single Alcatel-Lucent IP interface. The VRs must be in the same subnet.

Figure 33-3 shows a common VR setup in which associated routers provide mutual backup using VRRP. Router A forwards packets on IP address 10.1.1.1 to Hosts 1 and 2 on its default gateway. Router B forwards packets on IP address 10.1.1.2 to Host 3 on its default gateway. If Router A fails, VRID 1 uses IP address 10.1.1.1 to forward packets from Router B to Hosts 1 and 2. At the same time, the Router B interface is still configured to deliver packets on IP address 10.1.1.2 to Host 3. If Router B fails, VRID 2 forwards these packets through backup Router A.

Figure 33-3 Sample VRs



Master router

The VRRP master router, in either a normal or a failover situation, routes all IP packets into the LAN using the physical MAC address for the IP interface as the Layer 2 source MAC address. ARP packets also use the parent IP interface MAC address as the Layer 2 source MAC address.

Owner and non-owner VRRP instances

A VRRP instance is configured in either an owner or non-owner mode.

The owner instance controls the IP address of the VR and is responsible for forwarding packets sent to this IP address. The IP address of the owner VRRP instance is the same as the real interface IP address of the router. The owner assumes the role of the master VR when it is functioning normally in the network. Only one VRRP instance in the domain is configured as the owner. All other instances participating in the domain are non-owners and must have the same VRID.

A backup router becomes the master router after a failover and continues to use the IP address of the original master. As a result, the new master router is the IP address non-owner.

The most important parameter to define for a non-owner VRRP instance is the priority. The priority defines for a VR the selection order. The priority value and the preempt mode combine to determine which VR has the highest priority and becomes the master.

The base priority is used to derive the in-use priority of the VRRP instance as modified by an optional VRRP priority-control policy. VRRP priority-control policies are used to either override or adjust the base priority value depending on events or conditions in the NE. See chapter 47 for more information.

VRRP types

When you create a VR, you specify the VRRP type, for example, network or L3 service, and the VR instance is restricted to the specified VRRP type. Configuring a VR using a mix of network and service interfaces through CLI raises a configuration mismatch alarm.

Primary addresses

A primary IP address is an address that is selected from the set of real interface addresses on the VR. VRRP advertisements between master and backup VRRP instances are sent using the primary IP address as the source of the IP packet.

The 7450 ESS, 7750 SR, or 7950 XRS IP interface must always have an assigned primary IP address for VRRP to operate on the interface. The primary IP address of the VR and the primary address on the IP interface are always the same.

Backup addresses

A maximum of 16 IP addresses (for either IPv4 or IPv6) in different subnets can be configured for a VRRP instance. One backup address is permitted for a subnet. The number of backup addresses is limited to the number of primary and secondary addresses configured on the IP interface.

The backup IP addresses for the owner VRRP instance must match the primary address or one of the secondary addresses on the IP interface. If the VRRP instance is not the owner, the backup addresses must be in the subnets of the primary and secondary addresses of the IP interface.

The 5620 SAM includes only eligible IP addresses in the search list.

VRRP message authentication

The type of authentication used by the VR in VRRP advertisement is specified during VRRP instance creation. The current master router uses the configured authentication type when sending VRRP advertisements to backup routers, which authenticate the messages.

33.2 Workflow to configure VRRP

1. Before you create a VR, ensure that a primary IP address is configured for the network or L3 service interface. Each interface must have a primary IP address. See Procedure 22-10 for more information.
2. Configure the VRRP priority-control policy for a non-owner VRRP instance. See chapter 47 for more information about VRRP priority-control policy events.
3. Create the VR. See Procedure 33-1 for more information.
4. As required, create VRRP instances in the VR. See Procedure 33-2 for more information.

33.3 VRRP management procedures

Use the following procedures to perform VR creation and VRRP management tasks.

Procedure 33-1 To create a VR

1 Choose Manage→Networking→VRRP Virtual Routers from the 5620 SAM main menu. The Manage VRRP Virtual Routers form opens.

2 Click on the Create button. The Virtual Router (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Virtual Router ID
- Backup Address
- Name
- Description
- VRRP Type
- Subnet Mask

If you are creating an IPv6 VR, the Backup Address parameter value that you specify must be an IPv6 address.

4 Click on the OK button. The Virtual Router (Create) form closes.

Procedure 33-2 To create and configure a VRRP instance

Before you create a VRRP instance on an interface, ensure that the L3 service or network interface is configured with a primary IP address. The backup IP address that is configured in Procedure 33-1 must belong to the same subnet as the primary IP address of the owner VRRP instance created in this procedure. The 5620 SAM automatically configures a backup address using the IP address of the VR. A search of interface IDs in step 7 of this procedure displays the interface IDs that are eligible for the creation of a VRRP instance for the VR.

You can configure up to a total of four VRRP instances (IPv4 plus IPv6) on one IP interface. However, only one IPv6 instance can be included in this total. The maximum number of mixed IPv4 and IPv6 VRRP instances on an NE is 1024.

1 Choose Manage→Networking→VRRP Virtual Routers from the 5620 SAM main menu. The Manage VRRP Virtual Routers form opens.

2 Configure the filter criteria. A list of VRs is displayed at the bottom of the Manage VRRP Virtual Routers form.

3 Choose a VR and click on the Properties button. The Virtual Router (Edit) form opens with the General tab displayed.

4 Click on the Components tab.

5 Select and right-click on VR Instances and choose Create VRRP Instance from the contextual menu. The VRRP Instance (Create) form opens with the General tab displayed.



Note — If the Backup Address parameter value that you specified in step 3 of Procedure 33-1 is an IPv6 address, then the contextual menu item is Create VRRP IPv6 Instance, and the VRRP IPv6 Instance (Create) form opens.

6 Click on the Select button in the Interface panel. The Select Interface - VRRP Instance or Select Interface - VRRP IPv6 Instance form opens, depending on whether you are creating an IPv4 or IPv6 VRRP Instance respectively.

7 Use the configurable filter and Search button to choose an interface, and click on the OK button. The Select Interface - VRRP Instance (or Select Interface - VRRP IPv6 Instance) form closes and the VRRP Instance (Create) (or VRRP IPv6 Instance (Create)) form reappears with the interface information displayed.

8 Configure the parameters:

- Owner
- Administrative State
- Base Priority

9 If the Owner parameter in step 8 is set to true, you cannot configure the Administrative State and Base Priority parameters and you cannot associate a policy with this VRRP instance. Go to step 11.

10 Assign a VRRP policy to the instance, if required.



Note — The same VRRP policy can be applied to both IPv4 VRRP instances and IPv6 VRRP instances.

- Click on the Select button in the Policy panel. The Select VRRP Policy form opens.
- Choose a VRRP policy and click on the OK button. The Select VRRP Policy form closes and the VRRP Instance (Create) form reappears with the VRRP policy information displayed.

11 Click on the Behavior tab.

12 Configure the parameters:

- MAC Address
- Message Interval (seconds)
- Message Interval (milliseconds)
- Init Delay (seconds)
- Master Inherit Interval
- Ping Reply
- Telnet Reply
- Standby Forwarding
- Preempt Mode
- SSH Reply
- Traceroute Reply

13 If you require bidirectional forwarding detection for the VRRP instance, configure the Enable BFD Interface parameter, and then complete the following substeps:

i Click on the BFD Interface tab.

ii Click on the Select button beside the Service Name parameter and choose a service from the Select Service - BFD Interface form.

iii Click on the Select button beside the Interface Name parameter and choose a service from the Select Interface - BFD Interface form.

iv Configure the Destination Address parameter.

14 Click on the Authentication tab.

15 Configure the parameters:

- Type
- Init Delay (seconds)

16 Click on the Backup Addresses tab.

17 Click on the Create button. The Backup Address (Create) form opens.

18 Perform one of the following to configure backup addresses:

a Enter an IPv4 address (for an IPv4 VR) or IPv6 address (for an IPv6 VR) manually in the IP Address field in the Backup Address section.

b Select the IP address from a list:

i Click the Choose IP Address button adjacent to the IP Address field. The Select IP Address form opens.

ii Click on the Search button.

iii Choose the desired entry from the list.

iv Click on OK.

The Select IP Address form closes and the IP Address parameter is populated with your selection.

v Click on the Add Link Local Address button. The Admin Link Local Address defined for the network L3 access interface appears in the IP Address field.



Note — If you need to add the Link Local Address as a backup address, then the Admin Link Local Address must be configured and the Admin Link Local Address Preferred parameter must be enabled for the network L3 access interface that you are using. See Procedure 22-9 for more information.

19 Click on OK to save your changes and close the Backup Address (Create) form.

20 Click on the OK button. The Virtual Router (Edit) form reappears with the VRRP instances displayed in the VR instances tree.

Procedure 33-3 To add a VRRP instance

A VRRP instance that you add to the VR must have an IP address with the same VRID and subnet as those of the VR.

1 Choose Manage→Networking→VRRP Virtual Routers from the 5620 SAM main menu. The Manage VRRP Virtual Routers form opens.

2 Configure the filter criteria. A list of VRs is displayed at the bottom of the Manage VRRP Virtual Routers form.

3 Choose a VR and click on the Properties button. The Virtual Router (Edit) form opens with the General tab displayed.

4 Click on the Components tab.

5 Right-click on VR Instances and choose Add VRRP Instance.



Note — If you chose an IPv6 VR in step 3, the contextual menu item is Add VRRP IPv6 Instance, and the Select VRRP IPv6 Instance form opens.

The Select VRRP Instance form opens with a list of eligible instances.

6 Select an instance and click on the OK button. The Select VRRP Instance (or Select VRRP IPv6 Instance) form closes and the Virtual Router (Edit) form reappears with the interface information displayed.

Procedure 33-4 To modify a VR or VRRP instance

1 Choose Manage→Networking→VRRP Virtual Routers from the 5620 SAM main menu. The Manage VRRP Virtual Routers form opens.

2 Configure the filter criteria. A list of VRs is displayed at the bottom of the Manage VRRP Virtual Routers form.

3 Choose a VR and click on the Properties button. The Virtual Router (Edit) form opens with the General tab displayed.

4 Configure the VR parameters.

To configure parameters for a VRRP instance, click on the Components tab, select and right-click on the VRRP instance, and choose Properties from the contextual menu. Using the contextual menu, you can also:

- Configure the NE associated with the VRRP instance
- Configure the interface associated with the VRRP instance

5 Click on the Properties button in the Instance panel. The VRRP Instance (Edit) form opens with the General tab displayed.

6 The following tabs list the VRRP instance properties that you can select and configure:

- General—associations between the VRRP instance and NEs, network interfaces, and policies (non-owner VRRP instances only).
- Behavior—a virtual MAC address that must be the same for all participating VRRP instances
- Authentication—enables authentication of VRRP advertisements among participating VRRP instances in the VR. For more information, see "VRRP message authentication" in section 33.1.
- Backup Addresses—lists backup addresses, whose configuration options you can access by selecting a site and clicking on the Properties button. For more information, see "Backup addresses" in section 33.1.
- VR Instances—lists VRs, whose configuration options you can access by selecting a VR and clicking on the Properties button. For more information, see "Owner and non-owner VRRP instances" in section 33.1.

7 Modify the parameters for the VRRP instance as required.

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button to confirm the action. The VRRP Instance (Edit) form closes and the VR Instance (Edit) form reappears.

10 Click on the Close button to close the VR Instance (Edit) form.

Procedure 33-5 To view the status of a VR

The status of a VR informs you of potential problems, such as problems involving VR preconditions and operational states. You can view the following virtual status information:

- Aggregated Operational State—indicates the collective operational states of the VRRP instances in the VR, such as whether all instances are up, all instances are down, or one or more is down
- Number Of VRRP Instances—the number of owner and non-owner VRRP instances in the current VR
- Multiple Owners configured—one owner for each VR
- VR Instance(s) Down—one or more VRs are not working

- Backup Address Mismatch—the backup address for a VRRP instance does not match the primary IP address of the owner, and so does not match the VR IP address
- Only one instance configured—only one VR instance exists, either a master or backup; both are required
- Subnet Mismatch—the IP addresses of the owner and non-owner routers do not belong to the same subnet
- No Owner configured—an IP address owner is not assigned to the current VR

1 Choose Manage→Networking→VRRP Virtual Routers from the 5620 SAM main menu. The Manage VRRP Virtual Routers form opens.

2 Configure the filter criteria. A list of VRs is displayed at the bottom of the Manage VRRP Virtual Routers form.

3 Choose a VR and click on the Properties button. The Virtual Router (Edit) form opens with the General tab displayed. Status information is in the Status panel.

4 Click on the Close button to close the Virtual Router (Edit) form.

Procedure 33-6 To delete a VRRP instance

1 Choose Manage→Networking→VRRP Virtual Routers from the 5620 SAM main menu. The Manage VRRP Virtual Routers form opens.

2 Configure the filter criteria. A list of VRs is displayed at the bottom of the Manage VRRP Virtual Routers form.

3 Choose a VR and click on the Properties button. The Virtual Router (Edit) form opens with the General tab displayed.

4 Click on the Components tab.

5 Select and right-click on a VR instance and choose Delete from the contextual menu. A dialog box appears.

6 Click on the Yes button to confirm the action. The VR is deleted and removed from the VR instances tree.

7 Click on the Close button to close the Virtual Router (Edit) form.

Procedure 33-7 To delete a VR

1 Choose Manage→Networking→VRRP Virtual Routers from the 5620 SAM main menu. The Manage VRRP Virtual Routers form opens.

2 Configure the filter criteria. A list of VRs is displayed at the bottom of the Manage VRRP Virtual Routers form.

3 Choose a VR from the list.

4 Click on the Delete button. A dialog box appears.

5 Click on the Yes button to confirm the action. The VR is removed from the list.

6 Click on the Close button to close the Manage VRRP Virtual Routers form.

34 — APS

34.1 APS overview *34-2*

34.2 Workflow to manage APS *34-9*

34.3 APS management procedures *34-10*

34.1 APS overview

APS protects SONET/SDH lines from linear bidirectional failures. The NEs in a SONET/SDH network constantly monitor the health of the network. When a failure is detected, the network proceeds to transfer, or switch over, live traffic from the active, or working line, to the standby, or protection line. The transfer occurs quickly to minimize traffic loss. The traffic remains on the protection line until the fault on the working line clears, at which time the traffic can optionally revert to the working line.

In a 1+1 APS architecture, the active OC-*n* signal is transmitted to both the working and protection ports, so the same payloads are transmitted identically to the working and protection ports in the egress direction. The working and protection signals are selected independently in the ingress direction.



Caution — An NE transmits data only on the working line. For a single failure, this configuration can cause a delay of up to 100 ms during an APS switch.

In the 5620 SAM, the main APS elements are the following:

- APS groups

  An APS group is an aggregation of one or two SONET/SDH ports and the associated logical ports, known as APS channels. The first port is known as the working channel and must be configured in the APS group. The second port is the protection channel, which is optionally configurable. In a 1+1 optimized APS group, the protection channel is replaced with a second working channel.
- APS channels

  APS channels are logical and model the physical ports. The set of associated data for an APS channel includes the corresponding physical port identifier, the role, which is working or protection, and the name of the APS group to which the port belongs. If a protection channel is configured, it carries the traffic of the failed working channel. If the protection channel fails, the working channel carries the traffic.
- APS bundles

  APS bundles protect multilink PPP and IMA bundles on channelized ASAP MDAs. All the members of a working or protection APS bundle must belong to the same working or protection line of the APS group.
- APS common port configurations

  All SONET/SDH port parameters on the working and protection channels in an APS group must be identical except for the following:
  - Clock Source
  - Loopback
  - Report Alarms
  - BER Signal Degradation Threshold
  - BER Signal Failure Threshold
  - SONET Section Trace Mode

- APS commands
  Each APS channel has one APS operational command associated with it. The APS operational command is determined by the last command that is issued to both APS channels and the signal condition of the working and protection ports. APS commands affect the APS operational states but do not affect the configuration. The operational state does not persist through an NE restart.

Table 34-1 describes the events that affect 1+1 protection and their relative priority.

Table 34-1 Events affecting 1+1 protection

Priority	Event	Event type
1	Lockout of protection	User initiated
2	Signal failure on protection line	Automatically initiated
3	Forced switch	User initiated
4	Signal failure on working line	Automatically initiated
5	Signal degradation	Automatically initiated
6	Manual switch	User initiated
7	WTR time (revertive switching only)	User initiated (state request)
8	No reversion (non-revertive switching only)	User initiated (state request)

Consider the following when configuring APS.

- A port can belong to only one APS group.
- Two ports that belong to the same APS group must be of the same port type and have the same traffic speed.
- An APS group has one set of APS channels. The set can contain one or two APS channels.
- An APS channel can belong to only one APS group.
- A SONET/SDH port can either belong to only one APS channel.

Bidirectional mode

In 1+1 system bidirectional mode, a signal failure in either direction causes both the near-end and far-end NEs to switch to the protection channels. The highest-priority local request is compared with a remote request; the request that has the greater priority is selected. See Table 34-1 for the list of events that affect 1+1 protection.

Unidirectional mode

In a 1+1 system unidirectional mode, the working interface switches to the protection interface only for the direction in which a signal failure occurs. For example, if there is a signal failure in the transmit direction, the working interface switches to the protection interface for transmission but not for the receipt of data.

Switching modes

The following 1+1 system switching modes are available:

- non-revertive (default)
- revertive

In non-revertive switching, a switch to the protection channel is maintained even after the working line has recovered from a failure or a manual switch is cleared.

In revertive switching, the traffic is switched back to the working channel after the working line has recovered from a failure or a manual switch is cleared.

For revertive switching, you can define a period of time that the system must wait before it can restore traffic from the protection line to the working line. This delay, or WTR time, prevents frequent automatic switches from occurring as a result of intermittent failures.

In case of failure on both the working and protection lines, the line that has the less severe error remains active. If there is a signal degradation on both lines, the active line that failed last remains active. If there is a signal failure on both lines, the working line always remains active because a signal failure on the protection line is a higher priority than a signal failure on the working line.

MLPPP

MLPPP provides a way to distribute data across multiple links within an MLPPP APS bundle to achieve high bandwidth. MLPPP allows for a single frame to be fragmented and transmitted across multiple links. This reduces latency and allows for a higher maximum received recovery unit, or MRU.

MLPPP is supported in MC APS groups. See section "MC APS" for more information about MC APS.

Multiclass MLPPP

Multiclass MLPPP is an extension of the MLPPP standard which allows multiple classes of service to be transmitted over an MLPPP bundle.

Multiclass MLPPP changes the MLPPP header to include either two or four class bits to allow for up to either four or 16 classes of service. This allows multiple classes of services over a single MLPPP connection. The highest priority traffic is transmitted over the MLPPP bundle with minimal delay, regardless of the order in which packets are received.

Multiclass MLPPP is useful in mobile network deployments where multiple types of traffic, each with its own priority level, travel across a single MLPPP link bundle between the base station router and the aggregation router in the point of presence (POP) mobile operator.



Note — Multiclass MLPPP allows for several classes of services to be transmitted over an MLPPP bundle. Link fragmentation and interleaving, however, allows for only two classes of service to be transmitted. Multiclass MLPPP and link fragmentation and interleaving are mutually exclusive.

APS port configurations

A 7710 SR or 7750 SR network or access port can be connected to another 7710 SR or 7750 SR with both the working and protection channels on different IOMs in a single NE, or with the working channel on one NE and the protection channel on another.

Note — Mirroring parameters configured on a specific port or service are maintained during an APS failover.

All SONET/SDH MDAs support APS functionality. Table 34-2 lists the possible port pairings to provide APS protection. Both ports must be of the same type and have the same traffic speed.

Table 34-2 APS port configurations

MDA type—Working channel	MDA type—Protection channel
16 × OC12/OC3 SFP	8 × OC12/OC3 SFP or 16 × OC12/OC3 SFP
8 × OC12/OC3 SFP	8 × OC12/OC3 SFP or 16 × OC12/OC3 SFP
16 × OC3 SFP	8 × OC3 SFP or 16 × OC3 SFP
8 × OC3 SFP	8 × OC3 SFP or 16 × OC3 SFP
4 × OC48 SFP	2 × OC48 SFP or 4 × OC48 SFP
2 × OC48 SFP	2 × OC48 SFP or 4 × OC48 SFP
1 × OC192	1 × OC192
16 × ATM OC3 SFP	16 × ATM OC3 SFP
4 × ATM OC12/OC3 SFP	4 × ATM OC12/OC3 SFP
4 × Channelized OC3 ASAP	4 × Channelized OC3 ASAP
1 × Channelized OC12 ASAP	1 × Channelized OC12 ASAP
1 × Channelized OC3 CES	4 × Channelized OC3 CES
4 × Channelized OC3 CES	1 × Channelized OC3 CES
1 × Channelized OC12 CES	1 × Channelized OC12 CES

Note — The working and protection channels for the following MDA port pairs are set to the same traffic speed based on the APS group speed configuration:

- 16 × OC12/OC3 SFP and 16 × OC12/OC3 SFP
- 16 × OC12/OC3 SFP and 8 × OC12/OC3 SFP
- 8 × OC12/OC3 SFP and 16 × OC12/OC3 SFP
- 8 × OC12/OC3 SFP and 8 × OC12/OC3 SFP
- 4 × ATM OC12/OC3 SFP and 4 × ATM OC12/OC3 SFP

SC APS

1+1 APS can be implemented on a port-by-port basis. If all ports on an MDA or IOM need to be protected, the ports must be individually configured.

The working and protection lines are capable of being connected to:

- two ports on the same MDA
- two ports on different MDAs, and the MDAs are on the same IOM
- two ports on different MDAs on different IOMs

If the working channel and protection channel are on the same MDA, protection is limited to the physical port and the media that connect the two NEs. If different IOMs are used, protection extends to failure of each IOM.



Note — The working and protection channels should be configured on different MDAs but on the same IOM card for the 7705 SAR-8 and 7705 SAR-18, Release 6.0 R1 or later.

Working and protection lines can be connected to a 7450 ESS, 7710 SR, or 7750 SR, and serve as an access port that provides one or more services to the NE. The access port can be a single channel or multiple channels; each channel must support PPP. In the case of the ATM MDA, each channel must support ATM.

The end NE transmits a valid data signal to both the working and protection lines. The signal on the protection line is ignored until the working channel fails or degrades to the degree that requires a switchover to the protection channel. When the switchover occurs, all services, including all service QoS and filter policies, are activated on the protection channel.

The working channel on a 7750 SR, 7450 ESS, or 7710 SR, must connect to the working channel on a peer NE, and the protection channel on a 7750 SR, 7450 ESS, or 7710 SR, must connect to the protection channel on a peer NE.

1+1 optimized

You can configure an SC APS group with a 1+1 optimized configuration. A 1+1 optimized APS group is optimized for networks which rely primarily on 1+1 bidirectional switching. A 1+1 optimized APS group is configured with two working channels, as opposed to one working channel and one protection channel. In a 1+1 optimized configuration, one working channel acts as the primary channel, through which the traffic will always default. A 1+1 optimized APS group always operates in bidirectional and nonrevertive modes.

MC APS

You can use APS to protect against NE failure by configuring the working channel of an APS group on one 7705 SAR-8/18, 7750 SR, or 7710 SR, and configuring the protection channel of the same APS group on a different 7705 SAR-8/18, 7750 SR, or 7710 SR. The two NEs connect using an IP link that is used to establish a signaling path between them.

The working channel on the near-end NE must connect to the working channel on a peer NE, and the protection channel on the far-end NE must connect to the protection channel on a peer NE.

When an MC APS group is configured, the 5620 SAM automatically creates a container which aggregates the MC APS group configurations of each NE.

Multi-chassis APS configuration is supported for ATM clear channel interfaces.

APS on channelized ASAP MDAs

You can protect a channelized SONET/SDH port on a channelized ASAP MDA with a protection port of the same speed on a different channelized ASAP MDA in the same NE. The APS configuration on a channelized ASAP MDA provides protection against a port, MDA, or IOM failure. All SONET/SDH paths and TDM channels in a SONET/SDH port are protected.

Consider the following when you configure APS protection on a deep channel on a channelized ASAP MDA:

- Both SONET and SDH channels are supported.
- Up to three common configuration SONET channels can be created in an APS configuration.

APS on channelized CES MDAs

You can protect a channelized SONET/SDH port on a channelized CES MDA with a protection port of the same speed on a different channelized CES MDA in the same NE. The APS configuration on a channelized CES MDA provides protection against a port, MDA, or IOM failure. All SONET/SDH paths and TDM channels in a SONET/SDH port are protected.

Consider the following when you configure APS protection on a deep channel on a channelized CES MDA:

- Both SONET and SDH channels are supported.
- Up to three common configuration SONET channels can be created in an APS configuration.

APS on multilink bundles

APS on multilink bundles consists of a working and protection bundle which provide bidirectional APS protection to each other. The members of a working or protection multilink bundle must belong to the same working or protection line of the APS group. User traffic is not sent on the protection line.

The 5620 SAM supports APS on MLPPP and IMA bundles. In IMA bundles, IMA cells are sent on the protection line as a keep-alive signal during an APS switchover.

APS 1+1 configuration on the channelized MDA provides protection to all the channels on the protected SONET/SDH port and to all of the multilink bundles with member that links reside on the protected SONET/ SDH port.

APS bundles on multiple NEs

You can configure APS bundles to provide bidirectional APS protection across multiple NEs. MC APS bundles are supported on the 7750 SR and 7710 SR.

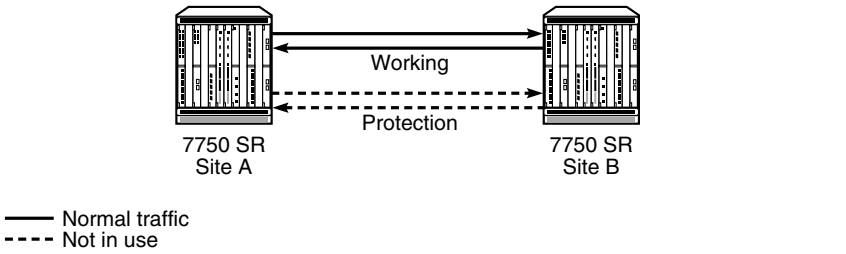
You can use APS to protect against failure by configuring the working bundle on one NE, and configuring the protection bundle of the same APS bundle group on a different NE. The two NEs connect to each other with an IP link that is used to establish a signaling path between them.

1+1 APS configuration example

Figures 34-1 and 34-4 show an example of 1+1 APS for two 7750 SRs that are configured for 1+1 APS in bidirectional and non-revertive modes.

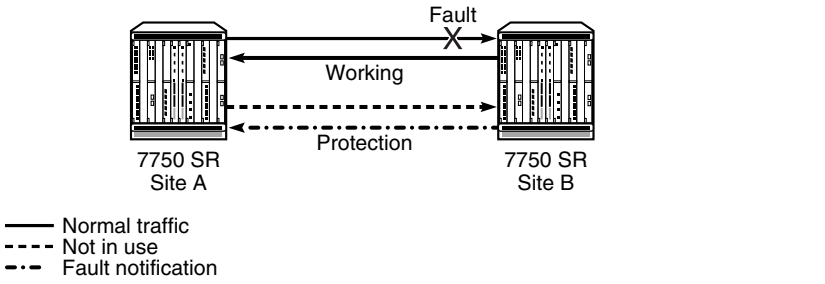
Figure 34-1 shows normal operations between two 7750 SRs. There are no faults on the working line, and the protection line is not in use.

Figure 34-1 Normal operations between two 7750 SRs



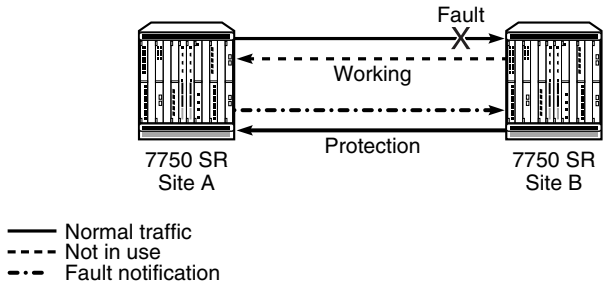
The working line degrades in the direction from site A to site B. Site B detects the fault and notifies site A of the fault using the protection line. Figure 34-2 shows the fault on the working line and site B notifying site A of the fault.

Figure 34-2 Site B detects the fault and notifies site A



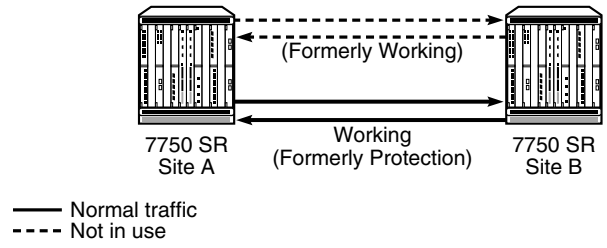
Site B automatically switches to the protection line. Site A receives the fault notification from site B and detects the fault on the working line. Site A acknowledges the fault and notifies site B that it is switching to the protection line. Figure 34-3 shows site B switching to the protection line and site A acknowledging the fault.

Figure 34-3 Site B switches to the protection line and site A acknowledges the fault



Site B receives the notification from site A and site A automatically switches to the protection line. Figure 34-4 shows normal operations resuming on the protection line between site A and site B. The protection line becomes and remains the working line since 1+1 APS is configured for non-revertive switching in this example.

Figure 34-4 Normal operations resume on the protection line



Configuring SAPs on APS-protected ports

You can use APS-protected ports to create SAPs for 5620 SAM services. The SAP list of a service creation form displays the APS-group SONET channels with all other SONET channels, but uses a different port ID format. An example of an APS group port ID is Channel aps-1.sts3-1. To create a SAP that uses an APS group, you must first configure the SONET channels in the APS group.

34.2 Workflow to manage APS

1 As required, create an SC APS group or MC APS group and configure the various channel types supported by APS groups. Configure the operational state for each APS channel. See Procedures 34-1 and 34-2 for more information.

2 As required, create an SC APS IMA or MLPPP bundle or MC APS MLPPP bundle. See Procedures 34-3 and 34-4 for more information.

3 As required, change the operational state of an APS channel; see Procedure 34-5.

4 As required, delete the APS group or bundle:

- See Procedure 34-6 to delete a SC APS group
- See Procedure 34-7 to delete a SC APS bundle
- See Procedure 34-8 to delete a MC APS group or bundle

34.3 APS management procedures

Use the following procedures to perform APS management tasks.

Procedure 34-1 To create an SC APS group

Perform this procedure to create an SC APS group and configure the various channel types supported by APS groups including:

- APS working channels
- APS protection channels
- APS SONET channels
- SONET clear channels
- The maximum number of channels on ports that support multiple sub-channels



Note — When a multiservice site is configured on an IOM, the working and protection ports must be configured on the same IOM.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

3 Right-click on the APS Groups object and choose Create APS Group from the contextual menu. The SC APS Group (Create) form opens with the General tab displayed.

4 Configure the Description parameter.

5 Click on the APS Group tab.

6 Configure the parameters:

- Auto-Assign ID
- Group Number
- APS Mode
- Direction
- Revert Mode
- Wait To Restore (seconds)
- Annex B Command Switch

7 Click on the States tab.

8 Configure the Administrative State parameter.



Note — When a working channel or protection channel is added to an APS group, the channel inherits the current administrative state of the APS group. After the channel is added to the APS group, the administrative state of the physical port can be changed independently.

9 Click on the Apply button. An SC APS Group icon appears under the APS Groups object in the navigation tree.

10 Click on the APS Group tab.

11 Configure the parameters, if applicable:

- Hold Time for Line Signal Degradation (100s of milliseconds)
- Hold Time for Line Signal Failure (100s of milliseconds)
- RDI Alarm Generation

12 Perform the following steps to configure the working and protection channels for the APS group.



Note 1 — Prior to completing this step, your NE device must be configured with a card that supports APS ports. See Table 34-2 for a list of cards the support APS ports.

Note 2 — To create an APS Working Channel, you can also right click on the SC APS Group icon under the APS Groups object in the navigation tree and choose Create APS Working Channel.

Note 3 — The working and protection channels should be configured on different MDAs but on the same IOM card for the 7705 SAR-8 and 7705 SAR-18, Release 6.0 R1 or later.

i Click on the APS Channels tab.

ii Click on the Create button. The APS Channel (Create) form opens.

iii Configure the Channel Role parameter, if applicable.



Note — If you are creating a 1+1 SC APS group, you must create the working channel before you create the protection channel.

iv Click on the Select button. The Select Port - APS Channel form opens.

v Click on the Search button. A list of available ports is displayed.

vi Select a port in the list and click on the OK button. The Select Port - APS Channel form closes.

vii Click on the OK button. The APS Channel (Create) form closes and a dialog box appears.

viii Click on the OK button. The channel is listed on the SC APS Group (Edit) form.

ix Repeat steps ii to viii to add the protection channel or second working channel.

x Click on the Apply button.

13 Configure the operational state of the working and protection channels. Perform the following steps:

i Choose a channel from the list and click on the Properties button. The APS Channel - *Type* (Edit) form opens with the APS Channel tab displayed.

ii Configure the Command Switch parameter.

iii Click on the OK button. The APS Channel - *Type* (Edit) form closes.

14 As required, configure the APS SONET channels for the APS group:

i Right-click on the SC APS Group icon in the navigation tree and choose Create APS SONET Channel from the contextual menu. The Sts1 SONET Channel (Create) form opens with the General tab displayed.

ii Configure the channels as described in Procedure 16-29.

15 Perform one of the following for the APS group:

a To create individual SONET clear channels:

i Right-click on the APS Common Config SONET channel icon and choose Create Channel from the contextual menu. The DSO Channel Group, (Create) form opens.

ii Configure the channel as described in Procedure 16-25.

b To create the maximum number of channels on ports that support multiple sub-channels:

i Right-click on the APS Common Config SONET channel icon and choose Create Maximum # of Channels from the contextual menu. The Create Maximum # of Channels form opens.

ii Configure the channels as described in Procedure 16-26.

Procedure 34-2 To create an MC APS group

Perform this procedure to create an MC APS group and configure the various channel types supported by APS groups including:

- APS working channels
- APS protection channels
- APS SONET channels

- SONET clear channels
- The maximum number of channels on ports that support multiple sub-channels

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC APS Group (APS) from the object drop-down list.

3 Click on the Create button. The MC APS Group (Create) form opens.

4 Configure the Group Number parameter.

5 Click on the Select button to configure the Site Id parameter in the First Element panel. The Select a Network Element list form opens.

6 Select an NE and click on the OK button. The Select a Network Element list form closes and the MC APS Group (Edit) form displays the system ID of the first NE in the MC APS group.

7 Click on the Select button to configure the Network Interface parameter in the First Element panel, if required. The Select a Network Element list form opens.



Note 1 — Only numbered IPv4 interfaces are listed.

Note 2 — The default interface is the NE system interface.

8 Click on the Select button to configure the Site Id parameter in the Second Element panel. The Select a Network Element list form opens.

9 Select an NE and click on the OK button. The Select a Network Element list form closes and the MC APS Group (Edit) form displays the system ID of the second NE in the MC APS group.

10 Click on the Select button to configure the Network Interface parameter in the Second Element panel, if required. The Select a Network Element list form opens.



Note 1 — Only numbered IPv4 interfaces are listed.

Note 2 — The default interface is the NE system interface.

11 Click on the Apply button. An MC APS Group Member icon appears under the APS Groups object in the navigation tree of the selected First Element and Second Element NEs.

12 Click on the Members tab to configure each MC APS group member.

13 Select a group member in the list and click on the Properties button. The MC APS Group Member (Edit) form opens with the General tab displayed.

14 Configure the Description parameter.

15 Click on the APS Group tab.

16 Configure the parameters:

- Revert Mode
- Wait To Restore (seconds)



Note — The Wait To Restore (seconds) parameter is configurable when the Revert Mode parameter is set to revertive.

17 Click on the States tab.

18 Configure the Administrative State parameter.



Note — When a working channel or protection channel is added to the APS group, the channel inherits the current administrative state of the APS group. After the channel is added to the APS group, the administrative state of the physical port can be changed independently.

19 Click on the Multi Chassis tab.

20 Configure the parameters:

- Advertise Interval (100s of milliseconds)
- Hold Time (100s of milliseconds)

21 Perform the following steps to configure the working and protection channels for the APS group.



Note — Prior to completing this step, your NE device must be configured with a card that supports APS ports. See Table 34-2 for a list of cards the support APS ports.

i Click on the APS Channels tab.

ii Click on the Create button. The APS Channel (Create) form opens.

iii Configure the Channel Role parameter.

iv Click on the Select button. The Select Port - APS Channel form opens.

v Click on the Search button. A list of available ports is displayed.

vi Select a port in the list and click on the OK button. The Select Port - APS Channel form closes.

vii Click on the OK button. The APS Channel (Create) form closes and a dialog box appears.

viii Click on the OK button. The channel is listed on the MC APS Group (Edit) form.

ix Repeat steps ii to viii to add the protection channel or second working channel.

x Click on the Apply button.

22 Configure the operational state of the working and protection channels. Perform the following steps:

i Choose a channel from the list and click on the Properties button. The APS Channel - *Type* (Edit) form opens with the APS Channel tab displayed.

ii Configure the Command Switch parameter.

iii Click on the OK button. The APS Channel - *Type* (Edit) form closes.

23 As required, configure the APS SONET channels for the APS group:

i Right-click on the MC APS Group icon in the navigation tree and choose Create APS SONET Channel from the contextual menu. The Sts1 SONET Channel (Create) form opens with the General tab displayed.

ii Configure the channels as described in Procedure 16-29.

24 Perform one of the following for the APS group:

a To create individual SONET clear channels:

i Right-click on the APS Common Config SONET channel icon and choose Create Channel from the contextual menu. The DSO Channel Group, (Create) form opens.

ii Configure the channel as described in Procedure 16-25.

b To create the maximum number of channels on ports that support multiple sub-channels:

i Right-click on the APS Common Config SONET channel icon and choose Create Maximum # of Channels from the contextual menu. The Create Maximum # of Channels form opens.

ii Configure the channels as described in Procedure 16-26.

Procedure 34-3 To create an SC APS IMA or MLPPP bundle

Perform this procedure to create an APS bundle using IMA or MLPPP links on one NE. Consider the following when you add a DS0 channel that is a member of an APS group to an APS bundle:

- An APS channel can be a member of an APS bundle only, not of an IMA or multilink PPP bundle.
- All members of a working bundle must belong to a working channel of the same APS group.
- All members of a protection bundle must belong to a protection channel of the same APS group.

- You must create the working bundle before you can add an APS member to the APS bundle. If the member has a protection port, you must create the protection bundle before you can add the member to the APS bundle.
- You cannot delete the working port member of an APS bundle until you remove the member from the APS bundle.

The rules for adding a member to a bundle that is part of an APS bundle also apply to adding a member to a non-APS protected multilink bundle. See Procedures 15-41 and 15-39 for more information.

The following restrictions apply when adding a DS0 channel to an IMA bundle:

- The Clock Source parameter must be set to Node Timed.
- The encapsulation type of the DS0 channel must be ATM.

The following restrictions apply when adding a DS0 channel to a PPP bundle:

- All time slots on the DS0 channel must be selected.
- The encapsulation type of the DS0 channel must be IPCP.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure APS bundle and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Right-click on the APS Bundles object and choose Create Bundle from the contextual menu. The APS Bundle Display form opens.

5 Configure the parameters:

- Bundle ID
- Auto-Assign ID
- Description

6 Click on the Next button.

7 Configure the parameters:

- Bundle Type

a If you set the Bundle Type parameter to IMA Group, configure the following parameters:

- Red Diff Delay (milliseconds)
- Minimum Links
- IMA Version
- ATM Interface Cell Format
- ATM Minimum VPI Value
- Test Pattern
- Link Activation Timer
- Link Deactivation Timer
- Maximum Links

b If you set the Bundle Type parameter to PPP, configure the following parameters:

- Fragment Threshold (bytes)
- Red Diff Delay (milliseconds)
- Red Diff Delay Action
- Minimum Links
- Yellow Diff Delay (milliseconds)
- Bundle MRRU (bytes)
- Short Sequence
- Link Fragmentation and Interleaving

8 Click on the Finish button.

9 Click on the Close button. The APS Bundle Display form closes.

10 If the Bundle Type parameter is set to PPP in step 7, perform the following steps to configure the MLPPP bundle for multiclass service transmission.



Note — Consider the following when you configure MC MLPPP.

- MC MLPPP is supported only on channelized ASAP MDAs in a 7750 SR or 7710 SR.
- You must configure MC MLPPP before you add bundle members.
- MC MLPPP is configured on the main APS bundle and the parameters are propagated to the working and protection bundles.

i Right-click on the SC APS Bundle object in the navigation tree and choose Properties from the contextual menu. The APS Bundles (Edit) form opens.

ii Click on the MLPPP tab.

iii Configure the parameters:

- End Point ID
- End Point Class ID
- Class Count
- Magic Number
- Stateless Aps Switchover

iv Click on the Select button in the MLPPP Ingress QoS Profile or MLPPP Egress QoS Profile panel to choose a QoS profile, if required. If a profile is already selected, click on the Clear button to clear the selection and enable the Select button. The Select MLPPP Ingress QoS Profile or Select MLPPP Egress QoS Profile form opens.



Note — You can only apply QoS profiles to an MC MLPPP bundle when the Class Count parameter is set to 4.

v Select a profile and click on the OK button. The Select MLPPP Ingress QoS Profile or Select MLPPP Egress QoS Profile form closes.

11 Click on the States tab.

12 Configure the Administrative State parameter.



Note — You must configure the End Point ID parameter on the APS PPP group before you set the Administrative State parameter to Up on the working and protection bundles.

13 Click on the OK button. A dialog box appears.

14 Click on the Yes button. The APS Bundles (Edit) form closes.

15 To configure the APS working and protection bundles, perform the following steps.



Note — You must create the working bundle before you create the protection bundle.

i Right-click on the SC APS Bundle icon in the navigation tree and choose Create APS Working Bundle from the contextual menu. The Create APS Working/Protecting Bundle form opens.

ii Configure the parameters:

- Bundle ID
- Auto-Assign ID
- Description
- Daughter Card CLI Name
- Administrative State

iii Click on the Next button to view the configured bundle parameters.

iv Click on the Finish button.

v Click on the Close button. The Create APS Working/Protecting Bundle form closes.

vi Right-click on the SC APS Bundle icon in the navigation tree and choose Create APS Protection Bundle from the contextual menu. The Create Working/Protecting Bundle form opens.

vii Repeat steps ii to v to create the APS protection bundle.

16 To configure the administrative state of the APS working and protection bundles, perform the following steps.



Note — You must configure the End Point ID parameter on the APS PPP group before you change the working or protection bundle state.

i Right-click on the working bundle object below the SC APS Bundle object in the navigation tree and choose Properties from the contextual menu. The Multilink Bundle (Edit) form opens.

ii Click on the States tab.

iii Configure the Administrative State parameter.

iv Click on the OK button. A dialog box appears.

v Click on the Yes button. The Multilink Bundle (Edit) form closes.

vi Right-click on the protection bundle object below the SC APS Bundle object in the navigation tree. and choose Properties from the contextual menu. The Multilink Bundle (Edit) form opens.

vii Repeat steps ii to v.

17 To add members to the APS bundle, perform the following steps.

i Right-click on the SC APS Bundle icon in the navigation tree and choose Create Bundle Members from the contextual menu. The Add Bundle Member form opens.

ii Click on the Next button to add DS0 channel groups to the bundle. The Select Channels form opens.

iii Select a compatible channel from the list.



Note 1 — When initially adding bundle members, you must first add one channel group and then repeat the procedure to select up to seven additional channel groups.

Note 2 — Only compatible channels are listed. If you want to configure and use a channel that is currently incompatible, you can click on the Back button, deselect the Show Only Compatible Channels parameter, click on the Next button, select the channel, click on the Properties button.

Note 3 — The channel group with the lowest Port ID is the primary member for the bundle. The Encap Type of the primary member is used for all other members. When adding members to a bundle at a later time, the Encap Type must be the same as the primary member Encap Type for the member to be compatible.

iv Click on the Finish button and confirm the action. The Add Bundle Member form closes.

v Click on the Apply button.

vi Click on the Add button. The Add Bundle Member form opens.

vii Configure the Show Only Compatible Channels parameter.

viii Click on the Next button. The Select Channels form opens.

ix Select up to seven additional channels from the list.

x Click on the Finish button. A dialog box appears.

xi Click on the Yes button. The Add Bundle Members form closes.

xii Click on the Finish button.

xiii Click on the Close button. The Add Bundle Member form closes.

Procedure 34-4 To create an MC APS MLPPP bundle

Perform this procedure to create an APS bundle using IMA or MLPPP links on two NEs.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC APS Bundles (Bundle) from the object drop-down list.

3 Click on the Create button. The MC APS Bundles (Create) form opens.

4 Configure the Bundle Number parameter.

5 Click on the Select button beside the First Network Element parameter. The Select a Network Element list form opens.

6 Select an NE in the list and click on the OK button. The Select a Network Element list form closes.

7 Click on the Select button beside the Second Network Element parameter. The Select a Network Element list form opens.

8 Select an NE in the list and click on the OK button. The Select a Network Element form closes.

9 Click on the OK button. An MC APS Bundle object appears in the navigation tree under the APS Bundles object of each specified NE.

10 Close the Manage Node Redundancy form.

11 Configure the MLPPP bundle for multiclass service transmission. Perform the following steps.



Note — Consider the following when you configure MC MLPPP.

- You must configure MC MLPPP before you add bundle members.
- MC MLPPP is configured on the main APS bundle and the parameters are propagated to the working and protection bundles.

i Right-click on the new MC APS Bundle object in the navigation tree and choose Properties from the contextual menu. The APS Bundles (Edit) form opens.

ii Click on the MLPPP tab.

iii Configure the parameters:

- End Point ID
- End Point Class ID
- Class Count
- Magic Number
- Stateless Aps Switchover

iv Click on the Apply button. A dialog box appears.

v Click on the Yes button.

12 Click on the States tab.

13 Configure the Administrative State parameter.



Note — You must configure the End Point ID parameter on the APS PPP group before you set the Administrative State parameter to Up on the working and protection bundles.

14 Click on the OK button. A dialog box appears.

15 Click on the Yes button. The APS Bundles (Edit) form closes.

16 Perform the following steps to configure the MC APS working and protection bundles.

i Right-click on the MC APS Bundle object created in step 6 in the navigation tree and choose Properties from the contextual menu. The APS Bundles (Edit) form opens.

ii Click on the Protection and Working Bundles tab.

iii Click on the Create button. The Create APS Working/Protecting Bundle form opens.

iv Configure the parameters:

- Bundle ID
- Auto-Assign ID
- Description
- Administrative State

v Click on the Select button beside the Daughter Card CLI Name parameter. The Select Daughter Card - Multilink Bundle list form opens.

vi Select a daughter card in the list and click on the OK button. The Select Daughter Card - Multilink Bundle list form closes.

vii Click on the Next button.

viii Configure the parameters.

- Bundle Type
- Protection Type

  The working bundle must be on the same NE as the APS working channel and the protection bundle must but on the same NE as the APS protection channel.

ix Click on the Finish button.

x Click on the Close button. The Create APS Working/Protecting Bundle form closes.

xi Close the APS Bundles (Edit) form.

xii Repeat steps i to xi to configure the MC APS protection bundle created in step 8.

17 Perform the following steps to configure the administrative state of the MC APS working and protection bundles.

i Right-click on the working bundle object in the navigation tree and choose Properties from the contextual menu. The Multilink Bundle (Edit) form opens.

ii Click on the States tab.

iii Configure the Administrative State parameter.

iv Click on the OK button. A dialog box appears.

v Click on the Yes button. The Multilink Bundle (Edit) form closes.

vi Right-click on the protection bundle object in the navigation tree and choose Properties from the contextual menu. The Multilink Bundle (Edit) form opens.

vii Repeat steps ii to v.

18 To add multilink bundle members, perform the following steps.

i Right-click on the MC APS Bundle object on either NE in the navigation tree and choose Properties from the contextual menu. The APS Bundles (Edit) form opens.

ii Click on the Bundle Members tab.

iii Click on the Add button. The Add Bundle Member form opens.

iv Configure the Show Only Compatible Channels parameter.

v Click on the Next button. The Select Channels form opens.

vi Select a channel in the list.



Note 1 — When initially adding bundle members, you must first add one channel group and then repeat the procedure to select up to seven additional channel groups.

Note 2 — Only compatible channels are listed. If you want to configure and use a channel that is currently incompatible, you can click on the Back button, deselect the Show Only Compatible Channels parameter, click on the Next button, select the channel, click on the Properties button.

Note 3 — The channel group with the lowest Port ID is the primary member for the bundle. The Encap Type of the primary member is used for all other members. When adding members to a bundle at a later time, the Encap Type must be the same as the primary member Encap Type for the member to be compatible.

vii Click on the Finish button. A dialog box appears.

viii Click on the Yes button. The Add Bundle Members form closes.

ix Click on the Apply button.

x Click on the Add button. The Add Bundle Member form opens.

xi Configure the Show Only Compatible Channels parameter.

xii Click on the Next button. The Select Channels form opens.

xiii Select up to seven additional channels from the list.

xiv Click on the Finish button A dialog box appears.

xv Click on the Yes button. The Add Bundle Members form closes.

xvi Click on the OK button. The APS Bundles (Edit) form closes.

Procedure 34-5 To change the operational state of an SC APS channel

1. Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.
2. Right-click on the device where you want to modify the APS channel and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.
3. On the Network Element (Edit) form navigation tree, expand the Shelf icon fully.
4. Right-click on the APS Channel object. The APS Channel (Edit) form opens.
5. Configure the Command Switch parameter.
6. Click on the OK button. A dialog box appears.
7. Click on the Yes button. The operational state of the APS channel changes and the APS Channel (Edit) form closes.

Procedure 34-6 To delete an SC APS group

1. Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.
2. Right-click on the device where you want to delete an APS group and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.
3. On the Network Element (Edit) form navigation tree, expand the Shelf icon.
4. Right-click on the APS Group object and choose Delete from the contextual menu. A dialog box appears.



Caution — Removing an APS group removes the working and protection channels and associated ports from the APS group, and deletes the APS group ID. Ensure that you select the correct APS group.

5. Click on the View Dependencies button. A dialog box appears.
6. Click on the OK button.

7 Select the I understand the implications of this action check box.

8 Click on the Yes button. The 5620 SAM deletes the SC APS group.

Procedure 34-7 To delete an SC APS bundle

Perform this procedure to permanently remove an SC APS bundle from the 5620 SAM and NE configurations.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to delete an APS bundle and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Right-click on the APS Bundle object and choose Delete from the contextual menu. A dialog box appears.

5 Click on the View Dependencies button. A dialog box appears.

6 Click on the OK button to proceed.

7 Select the I understand the implications of this action check box.

8 Click on the Yes button. The 5620 SAM deletes the SC APS bundle.

Procedure 34-8 To delete an MC APS group or bundle

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Perform one of the following.

   a Choose MC APS Group (APS) from the object drop-down list.

   b Choose MC APS Bundles (APS) from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of MC APS groups or MC APS bundles appears.

4 Select an entry in the list and click on the Delete button. A dialog box appears.

5 Click on the View Dependencies button. A dialog box appears.

6 View the dependency information.

7 Click on the OK button.

8 Select the I understand the implications of this action check box.

9 Click on the Yes button. The 5620 SAM deletes the MC APS group or bundle and the corresponding configuration on each member site.

35 — lightRadio Wi-Fi

35.1 lightRadio Wi-Fi *35-2*

35.2 Workflow to configure lightRadio Wi-Fi *35-4*

35.1 lightRadio Wi-Fi

To provide additional capacity and extended coverage to a network, the 5620 SAM supports the offloading of traffic to WLANs, also known as Wi-Fi Offload. Users within range of a WLAN access point can establish a secure connection using RADIUS authentication. WPA2 keys are provided by a RADIUS server. Data is then transmitted through a single GRE tunnel to the WLAN Gateway (GW), where a subscriber DHCP session is created. The WLAN GW supports a RADIUS proxy server, which stores all available information from the RADIUS access-accept message.

In cases where the RADIUS server instructs the WLAN GW to forward traffic to a GGSN, a mobile gateway (MG) peer is created on the NE. Read-only information relating to the MG peers can be viewed on a base routing instance configuration form, under the WLAN GW tab.

Wi-Fi access can be offered from:

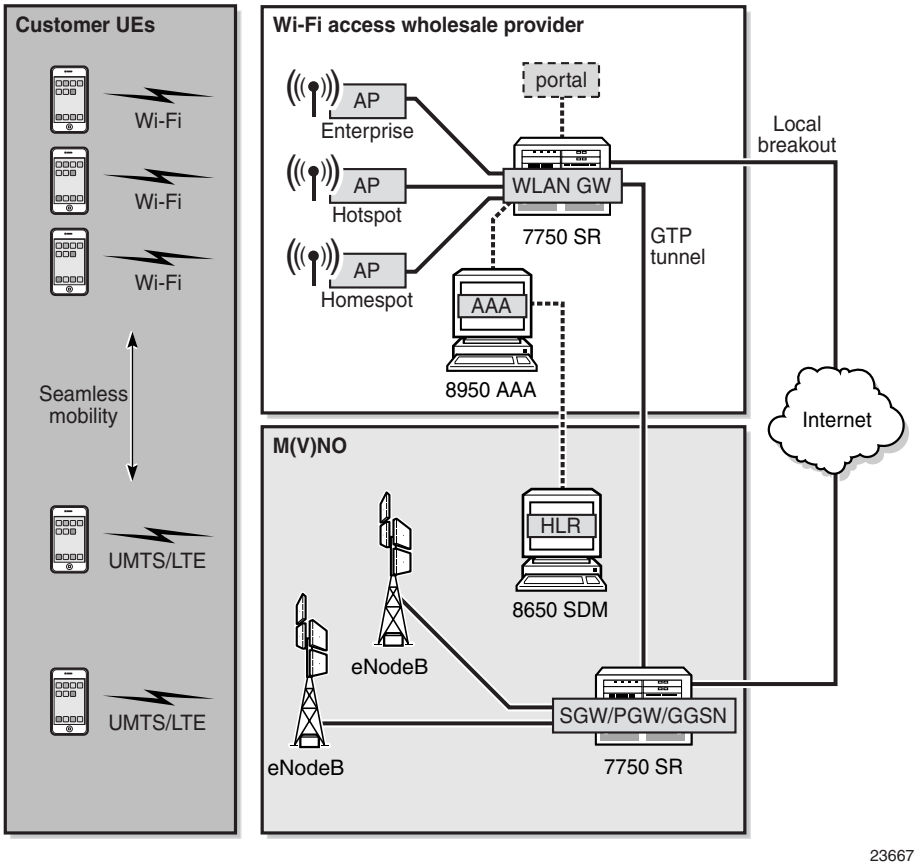
- hotspots - access points in public places.
- enterprise hotspots - access points in workplaces.
- homespots - access points on wireline CPEs from residential subscribers.

Wi-Fi access can be offered using the following SSID types:

- Private SSID - used by a residential subscriber to access wireline Internet service.
- Community SSID - used by visiting subscribers to access a Wi-Fi community broadband service after IEEE 802.1X authentication.
- Public SSID - used by visiting subscribers to access a free Internet service, or to access a Wi-Fi community broadband service after portal-based authentication.

Figure 35-1 shows a typical Wi-Fi Offload scenario. The UE attempts to switch over to Wi-Fi upon detection of a network SSID. Transparent IEEE 802.1X/EAP authentication takes place between the AP and UE. An optional GTP session can be established from the WLAN GW to the GGSN/PGW. This session is established dynamically so that UE traffic can be transferred back to an MMO.

Figure 35-1 Wi-Fi Offload



Migrant user handling

The 5620 SAM supports migrant user handling in a Wi-Fi offload application. Migrant users may have no intention of using the service, or may be invalid users who have failed authentication on the service. Both of these types of subscriber consume IP addresses and ESM resources on a WLAN GW. In a dormant subscriber handling model, the ESM subscriber is created on the IOM only when the following conditions are met:

- The subscriber is authenticated, either by RADIUS authentication or by MAC-based pre-authentication (where the RADIUS server remembers a previously authenticated UE).
- The subscriber is determined to be active by transmitting data beyond the initial DHCP request (data-triggered host creation).

Migrant user support works in conjunction with L2-aware NAT, where each UE is allocated the same inside IP address, and is assigned an outside address based on its subscriber ID (MAC address). In the case of L2-aware NAT and soft GRE, the address is assigned via DHCP, and each user is assigned the same lease. Migrant user handling is configured on an IES or VPRN soft GRE group interface, and includes the following functions:

- Data-triggered authentication and ESM host creation for ISA users.
- ESM host creation based on RADIUS COA request for portal-authenticated users.
- Migrant user DHCP performance.

  IP addresses are assigned on the ISA for L2-aware NAT (without ESM host). CPM-based DHCP is employed on a soft-GRE group interface without L2-aware NAT.

  An HTTP-redirect function is configured on the ISA.

35.2 Workflow to configure lightRadio Wi-Fi

The following workflow describes the sequence of high-level tasks required to configure and manage lightRadio Wi-Fi.

1. As required, configure a port policy to be bound to the ISA-WLAN GW group; see Procedure 43-21.
2. As required, configure a NAT RADIUS server policy to be bound to the ISA-WLAN GW group; see Procedure 49-2.
3. Configure an ISA-WLAN GW group; see Procedure 14-8.
4. As required, configure RADIUS proxy functionality:
   - **i** Configure RADIUS servers on a routing instance; see Procedure 22-7.
   - **ii** Configure RADIUS proxy servers on a routing instance; see Procedure 22-8.
   - **iii** Configure RADIUS server policies; see Procedure 49-4.
   - **iv** Configure RADIUS proxy caches; see steps 38 to 45 of Procedure 65-5.
5. Configure a WLAN GW for an IES or VPRN group interface; see Procedure 70-13 or Procedure 71-62.
6. Configure a mobile gateway profile; see Procedure 54-13.
7. Configure a WLAN GW for a routing instance or VPRN routing instance; see Procedure 22-1 or Procedure 71-19.
8. Configure DNS addresses on a VPRN routing instance; see Procedure 71-20.
9. Configure serving network information on an NE; see Procedure 13-16

36 — MC peer groups

36.1 MC peer groups overview *36-2*

36.2 Workflow to manage MC peer groups *36-3*

36.3 MC peer groups management procedures *36-3*

36.1 MC peer groups overview

An MC peer group is a 5620 SAM object that defines the relationship between two peer NEs to provide system redundancy in an Ethernet network. An MC peer group configuration includes a list of protocols and objects with state information that is to be synchronized between the peers.

The 7210 SAS-M, 7210 SAS-X, 7450 ESS, 7705 SAR, 7710 SR, 7750 SR, and 7950 XRS each support the creation of up to 20 MC peer groups using Ethernet ports in access mode. An MC peer group can contain one or more of the following child group objects:

- MC IPsec tunnel group—see chapter 37
- MC endpoint group—see chapter 38
- MC LAG group—see chapter 39
- MC synchronization group—see chapter 40
- MC ring group—see chapter 41
- MC mobile group—see the *5620 SAM LTE EPC User Guide*



Note 1 — You can create MC endpoints only on the 7450 ESS, 7710 SR, 7750 SR, and 7950 XRS.

Note 2 — You can create MC mobile groups only on the 7750 MG configured with an SGW interface.

Note 3 — You can create MC IPsec tunnel groups only on the 7450 ESS-4, 7450 ESS-6, 7450 ESS-6v, 7450 ESS-7, and 7450 ESS-12 in mixed mode and in chassis mode D, and on the 7750 SR-7, 7750 SR-12, and 7750 SR-12E in chassis mode D.

When you create a child group object, the 5620 SAM automatically creates the child group members using the peer objects in the MC peer group.

The 5620 SAM automatically discovers MC peers that are configured on managed NEs and creates an MC peer group if the source address of each peer matches the peer address of the other. If an MC peer address on an NE is changed after discovery, for example, using a CLI, the 5620 SAM deletes the MC peer group but does not delete the peer configuration on either NE. When the mismatch is corrected, the 5620 SAM recreates the MC peer group.

When the MC peer addresses match but the 5620 SAM detects another MC peer group configuration mismatch, the 5620 SAM raises an alarm and displays a check mark beside the Asymmetrical Configuration Detected indicator on the General tab of the MC Peer Group properties form. The alarm information includes the type of configuration mismatch. When the mismatch is corrected, the alarm and check mark clear.

You can configure node redundancy from the Manage Node Redundancy form as well as the NE properties form. When both NEs in an MC peer group are managed by the 5620 SAM, you can configure node parameters for the MC peer group and either peer from the Manage Node Redundancy form. When only one NE in the MC peer group is managed by the 5620 SAM, you can configure node redundancy parameters only for the managed peer and only from the NE properties form.

You can configure MC IPsec as a failover mechanism for IPsec tunnels between two 7750 SRs. MC IPsec provides protection for NE failure or MS-ISA failure. When the active peer fails, the IPsec tunnels failover to the standby peer without re-establishing the session. See chapter 37 for more information.

36.2 Workflow to manage MC peer groups

1 Create an MC peer group. See Procedure 36-1 for more information.

2 As required, configure an MC peer within an MC peer group. See Procedure 36-2 for more information.

3 As required, perform an on-demand protocol synchronization between MC peer group members. See Procedure 36-3 for more information.

36.3 MC peer groups management procedures

Use the following procedures to perform MC peer group management tasks.

Procedure 36-1 To configure an MC peer group

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Peer Group (Multi-Chassis) from the object drop-down menu.

3 Perform one of the following:

a Create an MC peer group by performing the following:



Note — At least one MC peer must be a 5620 SAM-managed NE. The 5620 SAM raises an alarm when an MC peer group contains an unmanaged NE.

i Click on the Create button. The MC Peer Group (Create) form opens.

ii Click on the Select button in the First Element panel to choose the first site for the peer group. The Select Site Info - MC Peer Group form opens.

iii Choose an NE in the list and click on the OK button. The Select Site Info - MC Peer Group form closes, and the site name and system IP address are displayed on the MC Peer Group (Create) form.

iv To specify an interface other than the NE system interface for MC peer communication, click on the Select button beside the Source Address parameter. The Select a Source Address form opens.



Note 1 — Only numbered, non-multicast IPv4 interfaces are listed.

Note 2 — You can also enter a valid interface IP address.

v Choose an interface in the list and click on the OK button. The interface address is listed on the MC Peer Group (Create) form.

vi Click on the Select button in the Second Element panel to choose the second site for the peer group. The Select Site Info - MC Peer Group form opens.

vii Choose an NE in the list and click on the OK button. The Select Site Info - MC Peer Group form closes, and the site name and system IP address are displayed on the MC Peer Group (Create) form.

viii To specify an interface other than the NE system interface for MC peer communication, click on the Select button beside the Source Address parameter. The Select a Source Address form opens.



Note 1 — Only numbered, non-multicast IPv4 interfaces are listed.

Note 2 — You can also enter a valid interface IP address.

ix Choose an interface in the list and click on the OK button. The interface address is listed on the MC Peer Group (Create) form.

x Click on the Apply button. The MC Peer Group (Create) form refreshes with additional tabs.

xi Go to step 4.

b Configure an MC peer group.

i Configure the filter criteria and click on the Search button. A list of MC peer groups is displayed.

ii Choose an MC peer group and click on the Properties button. The MC Peer Group (Edit) form opens with the General tab displayed.

4 Configure the following parameters in the First Element panel:

- Peer Name
- Description
- Authentication Key
- Administrative State

If you do not configure the Peer Name parameter, the peer IP address is used by the MC endpoint.

5 Configure the following parameters in the Second Element panel:

- Peer Name
- Description
- Authentication Key
- Administrative State

If you do not configure the Peer Name parameter, the peer IP address is used by the MC endpoint.

6 To configure MC IPsec, see Procedure 37-1.

7 Click on the Peer Synchronization tab.

8 Configure the parameters:

- Sync Administrative State
- IGMP
- IGMP Snooping
- Subscriber IPoE Management
- Subscriber PPPoE Management
- SRRP
- MC Ring
- MLD Snooping
- MC Ring
- Subscriber Host Tracking
- MC IPsec
- MC Local DHCP Server



Note — See chapter 37 for more information about MC IPsec.

9 Click on the Associated Groups tab.

10 Create an MC LAG, if required.

i Right-click on the MC LAG object in the components tree and choose Create MC LAG from the contextual menu. The MC LAG (Create) form opens.

ii Perform steps 7 to 11 in Procedure 39-1.

11 Create an MC synchronization group, if required.

i Right-click on the MC Sync Group object in the components tree and choose Create MC Sync Group from the contextual menu. The MC Sync Group (Create) form opens.

ii Perform steps 6 to 12 in Procedure 40-1.

12 Create an MC Ring Group, if required.

i Right-click on the MC Ring Group object in the components tree and choose Create MC Ring Group from the contextual menu. The MC Ring Group (Create) form opens.

ii Configure the Name parameter.

iii Click on the Select button beside the Synchronization Tag parameter. The Select Multi-Chassis Sync Group form opens.

iv Choose an MC synchronization group from the list and click on the OK button. The Select Multi-Chassis Sync Group form closes and the MC synchronization group is displayed on the MC Ring Group (Create) form.

13 Create an MC endpoint group, if required.

i Right-click on the MC Endpoint Group object in the components tree and choose Create Endpoint Group from the contextual menu. The MC Endpoint Group (Create) form opens.

ii Perform steps 8 to 11 in Procedure 38-1.

14 Create an MC mobile group, if required. See the *5620 SAM LTE EPC User Guide*.

15 Click on the OK button. The MC Peer Group (Create) form closes.

16 Close the Manage Node Redundancy form.

Procedure 36-2 To configure an MC peer

Perform this procedure to modify an MC peer when there is a configuration mismatch with the other peer in an MC peer group.



Note — The MC peer parameters are configurable only when there is a configuration mismatch, which is indicated when the Neighbor Match check box on the MC Peer (Edit) form is unselected.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Peer Group (Multi-Chassis) from the object drop-down menu.

3 Configure the filter criteria and click on the Search button. A list of MC peer groups is displayed.

4 Choose an MC peer group and click on the Properties button. The MC Peer Group (Edit) form opens with the General tab displayed.

5 Click on the Members tab.

6 Choose an entry in the list and click on the Properties button. The MC Peer (Edit) form opens with the General tab displayed.

7 Configure the parameters:

- Description
- Source Address
- Authentication Key
- Administrative State

8 Configure the MC LAG group parameters.

i Click on the MC LAG tab.

ii Configure the parameters:

- Keep-Alive Interval (deciseconds)
- Lost Connection Wait Interval
- Administrative State

9 Configure the MC synchronization group parameters.

i Click on the Synchronization Protocol tab.

ii Choose an entry in the list and click on the Properties button. The MC Sync (Edit) form opens with the General tab displayed.

iii Configure the parameters:

- Synchronize IGMP
- Synchronize IGMP-Snooping
- Synchronize Subscriber Management
- Synchronize SRRP
- Synchronize MC Ring
- Synchronize MLD Snooping
- Synchronize Subscriber Host Tracking

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The MC Sync (Edit) form closes.

12 Close the MC Peer (Edit) form.

13 Close the MC Peer Group (Edit) form.

14 Close the Manage Node Redundancy form.

Procedure 36-3 To perform an on-demand protocol synchronization between MC peer group members

Perform this procedure to distribute the most recent protocol synchronization configuration to each member of an MC peer group. This is required when the configurations do not match, for example, after the configuration is changed locally on only one MC peer using a CLI. When the peer configurations do not match, the 5620 SAM raises an alarm and displays a check mark beside the Asymmetrical Configuration Detected indicator on the General tab of the MC Peer Group properties form.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Peer Group (Multi-Chassis) from the object drop-down menu and click on the Search button. A list of MC peer groups is displayed.

3 Choose an MC peer group in the list and click on the Properties button. The MC Peer Group (Edit) form opens with the General tab displayed.

4 Click on the Peer Synchronization tab.

5 Click on the Resync button to synchronize the member configurations.

6 Close the MC Peer Group (Edit) form.

7 Close the Manage Node Redundancy form.

Procedure 36-4 To view an MC peer on one NE

Perform this procedure to view an MC peer when only one NE in the MC peer group is managed by the 5620 SAM.



Note — This procedure assumes that you have already configured an MC peer group. If only one NE is managed by the 5620 SAM, you must create this object from the CLI.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the NE where you need to view an MC peer and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Redundancy tab.

4 Click on the MC Peer tab.

5 Configure the filter criteria, if required, and click on the Search button.

6 Choose an MC Peer in the list and click on the Properties button. The MC Peer (Edit) form opens with the General tab displayed.

7 View the information, as required.

8 Close the MC Peer (Edit) form.

9 Close the Network Element (Edit) form.

Procedure 36-5 To delete an MC peer group



Caution — Deleting an MC peer group removes all of the MC configurations that are associated with the MC peer group, such as the following:

- MC LAG groups
- MC synchronization groups
- MC ring groups

Ensure that you specify the correct MC peer group for deletion in this procedure.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Peer Group (Multi-Chassis) from the object drop-down menu.

3 Configure the filter criteria and click on the Search button. A list of MC peer groups is displayed.

4 Choose one or more MC peer groups in the list and click on the Delete button. A dialog box appears.

5 Click on the View Dependencies button. A Warning form opens.

6 View the dependency information.

7 Select the I understand the implications of this action check box.

8 Click on the Yes button. The 5620 SAM deletes the MC peer group and the corresponding configuration on each member site.

9 Close the Manage Node Redundancy form.

37 — MC IPsec

37.1 MC IPsec overview *37-2*

37.2 Workflow to configure and manage MC IPsec *37-2*

37.3 MC IPsec management procedures *37-3*

37.1 MC IPsec overview

MC IPsec provides a stateful failover mechanism for IPsec tunnels between two 7750 SRs—an active NE and a standby NE. Stateful failover allows IPsec traffic to continue to be forwarded without interruption if a failure occurs. MC IPsec provides protection for NE or MS-ISA failure. If an active NE fails, the IPsec tunnels failover to the standby peer without needing to re-establish the session. The failover mechanism can occur at the tunnel group level. A tunnel group can failover to the standby NE, independently of other tunnel groups on the active NE.

A mastership protocol is used to elect the active NE peer. The 5620 SAM synchronizes IPsec configuration states between the active and standby peers so that existing tunnels do not need to be re-established when a switchover occurs. The IPsec traffic is sent to the active NE peer using an IPsec route policy that exports IPsec routes to the routing protocol. The route metric is then changed according to the changes in active and standby roles.

You can view the role of a peer in an MC IPsec tunnel group by verifying the Master State indicator on the MC IPsec Group configuration form. The states are:

- Not Eligible—no election and not eligible for mastership
- Eligible—no election but eligible for mastership
- Discovery—no election during initial peer discovery interval
- Master—communicating with MC peer, elected active
- Standby—communicating with MC peer, elected standby

MC IPsec only supports IKEv2 static LAN-to-LAN tunnel. MC IPsec is supported only on the 7450 ESS-4, 7450 ESS-6, 7450 ESS-6v, 7450 ESS-7, and 7450 ESS-12 in mixed mode and in chassis mode D, and on the 7750 SR-7, 7750 SR-12, and 7750 SR-12E in chassis mode D. MC IPsec peers must be the same NE type. For example, the NEs in an MC peer group must both be 7750 SRs or 7450 ESSs.

You can use the 5620 SAM to create MC IPsec non-forwarding events on VRRP policies to track the MEP state of MC IPsec-based static routes. See Procedure 47-1 for more information.

IPsec VPN does not support redundancy.

37.2 Workflow to configure and manage MC IPsec

The following workflow describes the high-level steps required to configure MC IPsec.

1 Configure the ISA tunnel MDAs on both MC IPsec peer sites. See Procedure 14-5. You must:

   - enable the Multiple Active ISA Support parameter
   - enable the IPsec Responder Only parameter to configure the NE to act as an IKE responder when an MC IPsec switchover occurs and to not initiate a new SA policy or rekey an existing SA
   - ensure that the ISA tunnel groups have the same configuration on each MC IPsec peer site

Alternatively, you can create ISA tunnel groups when you configure the MC IPsec group in Procedure 37-2.

2 Enable MC IPsec on the MC peer group. See Procedure 37-1.

3 Ensure that peer group synchronization is enabled for MC IPsec. See Procedure 37-1.

4 Create an MC IPsec tunnel group between the MC peer NEs. See Procedure 37-2.

5 Configure MC IPsec parameters on:

- tunnel interfaces on a VPRN. See Procedure 37-3.
- L3 access interfaces on an IES or VPRN. See Procedure 37-4.

6 Configure two identical static IPsec tunnels using the redundant tunnel group on the two MC peer sites. You can create multiple IPsec tunnels on the same tunnel group. The IPsec tunnels must have the same tunnel names, tunnel properties, and associated IKE, transform, and security policies for redundancy to be possible. Tunnels with a mismatched configuration on one of the peers are lost when a switchover occurs. See Procedure 29-7.

7 Configure IPsec protocol and state parameters in the From Criteria of a routing policy statement entry. See Procedure 22-15.

i Set the Protocol parameter to IPsec.

ii Set the State parameter to one of the following:

- IPsec Master with Peer—The corresponding tunnel group is the master with a reachable peer.
- IPsec Master No Peer—The corresponding tunnel group is the master with an unreachable peer.
- IPsec Non Master—The corresponding tunnel group is not the master.

8 If required, perform a manual switchover from the MC IPsec tunnel group and from all of the associated IPsec tunnels that are configured above the MC IPsec tunnel group. See Procedure 37-5.

37.3 MC IPsec management procedures

Use the following procedures to perform MC IPsec management tasks.

Procedure 37-1 To configure MC IPsec on an MC peer group



Note 1 — MC IPsec is supported only on the 7450 ESS-4, 7450 ESS-6, 7450 ESS-6v, 7450 ESS-7, and 7450 ESS-12 in mixed mode and in chassis mode D, and on the 7750 SR-7, 7750 SR-12, and 7750 SR-12E in chassis mode D.

Note 2 — The MC IPsec peers must be of the same NE type. For instance, the NEs in an MC peer group must both be 7750 SRs or 7450 ESSs.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Peer Group (Multi-Chassis) from the object drop-down menu.

3 Configure the filter criteria and click on the Search button. A list of MC peer groups is displayed.

4 Choose an MC peer group and click on the Properties button. The MC Peer Group (Edit) form opens with the General tab displayed.

5 Configure the Enable MC IPsec parameter.

6 Click on the Apply button. The form refreshes with the MC IPsec peer site information and additional tabs.

7 Configure the first peer site, if required.

   i Click on the Properties button next to the First Peer Site ID parameter in the MC IPsec panel. The MC IPsec (Edit) form opens with the General tab displayed.

   ii Configure the parameters:

   - Keep-Alive Interval (deciseconds)
   - Lost Connection Wait Multiplier
   - Discovery Interval (seconds)
   - Post-Boot Discovery Interval (seconds)
   - Enable BFD

   iii Click on the OK button. The MC IPsec (Edit) form closes.

8 Configure the second peer site, if required.

i Click on the Properties button next to the Second Peer Site ID parameter in the MC IPsec panel. The MC IPsec (Edit) form opens with the General tab displayed.

ii Configure the parameters:

- Keep-Alive Interval (deciseconds)
- Lost Connection Wait Multiplier
- Discovery Interval (seconds)
- Post-Boot Discovery Interval (seconds)
- Enable BFD

iii Click on the OK button. The MC IPsec (Edit) form closes.

9 Click on the Peer Synchronization tab.

10 Configure the MC IPsec parameter to enable peer group synchronization for MC IPsec.

11 Click on the Re-Synchronize button.

12 Close the MC Peer Group (Edit) form.

13 Close the Manage Node Redundancy form.

Procedure 37-2 To create an MC IPsec group

Perform this procedure to create an MC IPsec group of ISA tunnels. You can create up to 16 MC IPsec groups on each MC peer site.



Note 1 — You must first assign an ISA tunnel group to each MC peer site. You must enable the Multiple Active ISA Support parameter on each ISA tunnel group for MC IPsec. You can create ISA tunnel groups when you configure the MC IPsec peer groups.

Alternatively, you can create ISA tunnel groups on the peer NEs before you perform this procedure. See Procedure 14-5.

Note 2 — You must first ensure that MC IPsec is enabled on the MC peer group and ensure that the peers are configured for MC IPsec. See Procedure 37-1 for more information.

Note 3 — An MC IPsec group can exist only when there is a member pair of MC IPsec tunnel groups between MC peer NEs. If one member of a tunnel group is deleted or changed from one peer NE, the 5620 SAM global MC IPsec group is also deleted or changed.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Peer Group (Multi-Chassis) from the object drop-down menu and click on the Search button. A list of MC Peer Groups is displayed.

3 Choose an MC peer group and click on the Properties button. The MC Peer Group (Edit) form opens with the General tab displayed.

4 Click on the Associated Groups tab.

5 Right-click on the MC IPsec Group object in the components tree and choose Create MC IPsec Group from the contextual menu. The MC IPsec Group (Create) form opens.

6 Configure the Synchronization Tag parameter.

7 Configure the MC IPsec tunnel group for the first NE in the MC IPsec Tunnel Group on First Site panel.

   i Click on the Select button beside the Tunnel Group ID parameter. The Select First Peer ISA Tunnel Group - MC IPsec Group list form opens with a list of ISA tunnel groups. If you do need to create a tunnel group, go to step viii.

   ii Click on the Create button. The ISA-Tunnel Group (Create) form opens with the General tab displayed.

   iii Configure the parameters:

   - Group Number
   - Description
   - Reassembly (msec)
   - Administrative State

   iv Enable the Multiple Active ISA Support and IPsec Responder Only parameters.

v Configure the Required Number of Active MDAs parameter.

vi Click on the OK button. The ISA-Tunnel Group (Create) form closes and the Select First Peer ISA Tunnel Group - MC IPsec Group form reappears.

vii Click on the Search button to refresh the list.

viii Choose a tunnel group and click on the OK button. The Select First Peer ISA Tunnel Group - MC IPsec Group form closes and the MC IPsec Group (Create) form refreshes with the tunnel group information.

ix Configure the parameters:

- Administrative State
- Priority

8 Configure the MC IPsec tunnel group for the second NE in the MC IPsec Tunnel Group on Second Site panel.

i Click on the Select button beside the Tunnel Group ID parameter. The Select Second Peer ISA Tunnel Group - MC IPsec Group list form opens with a list of ISA tunnel groups. If you do need to create a tunnel group, go to step viii.

ii Click on the Create button. The ISA-Tunnel Group (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Group Number
- Description
- Reassembly (msec)
- Administrative State

iv Enable the Multiple Active ISA Support and IPsec Responder Only parameters.

v Configure the Required Number of Active MDAs parameter.

vi Click on the OK button. The ISA-Tunnel Group (Create) form closes and the Select Second Peer ISA Tunnel Group - MC IPsec Group form reappears.

vii Click on the Search button to refresh the list.

viii Choose a tunnel group and click on the OK button. The Select Second Peer ISA Tunnel Group - MC IPsec Group form closes and the MC IPsec Group (Create) form refreshes with the tunnel group information.

ix Configure the parameters:

- Administrative State
- Priority

9 Click on the OK button. The MC IPsec Group (Create) form closes.

10 Close the MC Peer Group (Edit) form.

11 Close the Manage Node Redundancy form.

Procedure 37-3 To configure MC IPsec on a VPRN tunnel interface

Perform this procedure to configure MC IPsec to move traffic to the master NE in the event the standby NE receives traffic.



Note — The port configured on the tunnel must be created with a tunnel SAP. For example, tunnel-x.private/public:y. See Procedure 29-6 for more information.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the list filter parameters and click on the Search button. A list of services appears at the bottom of the Manage Services form.

3 Choose a VPRN service.

4 Click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

5 Click on the Tunnel Interfaces tab.

6 Choose a tunnel interface and click on the Properties button. The Tunnel Interface (Edit) form opens with the General tab displayed.

7 Configure the parameters:



Note — The next hop address that you specify is used by the standby NE to shunt traffic to the master NE in the event that the standby receives traffic. The next hop address is resolved in the routing table of the corresponding service.

- Redundant Next-Hop IP Address for Static ISA Tunnels
- Redundant Next-Hop IP Address for Dynamic ISA Tunnels

8 Click on the OK button. A dialog box appears.

9 Click on the OK button. The Tunnel Interface (Edit) form closes and the VPRN Service (Edit) form reappears.

10 Close the Manage Services form.

Procedure 37-4 To configure MC IPsec on an IES or VPRN L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES or VPRN service.

4 Click on the Properties button. The IES Service (Edit) form or the VPRN Service (Edit) form opens with the General tab displayed.

5 On the navigation tree, expand the Sites icon and the site on which you need to configure MC IPsec on the L3 access interface.

6 Perform one of the following.

a Create an L3 access interface on the IES or VPRN site. See Procedure 70-17 or Procedure 71-22.



Note — Ensure that the port you select for the interface is created with a tunnel SAP. For example, tunnel-x.private/public:y.

b Configure an IES or VPRN L3 access interface:

i Expand the Sites icon in the service navigation tree.

ii Expand the Sites icon on the IES or the Routing Instance icon on the VPRN.

iii Expand the Access Interfaces icon, right-click on the L3 access interface you need to configure and choose Properties from the contextual menu. The IES L3 Access Interfaces (Edit) or VPRN L3 Access Interfaces (Edit) form opens with the General tab displayed.

7 Configure MC IPsec, if required. Configure the parameters:

- Redundant Next-Hop IP Address for Static ISA Tunnels
- Redundant Next-Hop IP Address for Dynamic ISA Tunnels



Note 1 — The parameters are configurable only when the port on the interface is created with a tunnel SAP. For example, tunnel-x.private/public:y.

Note 2 — The next hop address that you specify is used by the standby NE to shunt traffic to the master NE if the standby receives traffic. The next hop address is resolved in the routing table of the corresponding service.

8 Click on the OK button. The IES L3 Access Interface (Edit) or VPRN L3 Access Interface (Edit) form form closes, and the IES Site (Edit) or VPRN Site (Edit) form reappears with the new interface information displayed in the service navigation tree.

9 Close the IES Site (Edit) or VPRN Site (Edit) form.

10 Close the IES Service (Edit) or VPRN Service (Edit) form.

11 Close the Manage Services form.

Procedure 37-5 To perform an MC IPsec switchover

Perform this procedure to perform a manual switchover from the MC IPsec tunnel group and from all of the associated IPsec tunnels that are configured above the MC IPsec tunnel group.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC IPSec Group (Multi-Chassis) from the object drop-down menu and click on the Search button. A list of MC IPSec groups is displayed.

3 Choose an MC IPsec group and click on the Properties button. The MC IPSec Group (Edit) form opens with the General tab displayed.

4 Click on the Components tab.

5 Right-click on the MC IPsec Group site object in the components tree and choose Properties from the contextual menu. The MC IPsec Tunnel Group (Edit) form opens with the General tab displayed.

6 Perform one of the following:

a When the Last Tunnel Group Switch Status in the Protection Status panel for the group is Nominal, click on the Perform Manual Switch button.

b When the Last Tunnel Group Switch Status in the Protection Status panel for the group is Not Ready, you cannot perform the switchover because of one or more of the following:

- there is no elected standby peer
- the synchronization of pending IPsec states must occur
- IKE states are pending download to ISAs

Go to step 7.

7 Close the MC IPSec Tunnel Group (Edit) form.

8 Close the MC IPSec Group (Edit) form.

9 Close the Manage Node Redundancy form.

Procedure 37-6 To view an MC IPsec peer on an NE

Perform this procedure to view an MC IPsec peer when only one NE in the MC IPsec peer group is managed by the 5620 SAM.



Note — This procedure assumes that you have already configured an MC IPsec peer group. If only one NE is managed by the 5620 SAM, you must create this object from the CLI.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the NE where you want to view an MC IPsec peer and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Redundancy tab.

4 Click on the MC Peer tab.

5 Configure the filter criteria, if required, and click on the Search button.

6 Choose an MC Peer in the list and click on the Properties button. The MC Peer (Edit) form opens with the General tab displayed.

7 Click on the MC IPsec tab.

8 Choose an MC IPsec peer in the list and click on the Properties button. The MC IPsec (Edit) form opens with the General tab displayed.

9 View the information, as required.

10 Close the MC IPsec (Edit) form.

11 Close the MC Peer (Edit) form.

12 Close the Network Element (Edit) form.

Procedure 37-7 To configure an MC IPsec peer site

You must ensure that any tunnel groups that are configured on the peer sites are administratively down.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Peer Group (Multi-Chassis) from the object drop-down menu.

3 Configure the filter criteria and click on the Search button. A list of MC peer groups is displayed.

4 Choose an MC peer group and click on the Properties button. The MC Peer Group (Edit) form opens with the General tab displayed.

5 Configure the first peer site, if required.

i Click on the Properties button next to the First Peer Site ID parameter in the MC IPsec panel. The MC IPsec (Edit) form opens with the General tab displayed.

ii Click on the Tunnel Groups tab.

iii Choose a tunnel group and click on the Properties button. The MC IPsec Tunnel Group (Edit) form opens with the General tab displayed.

iv Set the Administrative State parameter to Down.

v Click on the OK button. A dialog box appears.

vi Click on the Yes button. The MC IPsec Tunnel Group (Edit) form closes.

vii Repeat steps iii to vi to set the Administrative State parameter to Down for additional tunnel groups, if required.

viii Click on the General tab.

ix Configure the parameters:

- Keep-Alive Interval (deciseconds)
- Lost Connection Wait Multiplier
- Discovery Interval (seconds)
- Post-Boot Discovery Interval (seconds)
- Enable BFD

x Click on the OK button. A dialog box appears.

xi Click on the Yes button. The MC IPsec (Edit) form closes.

6 Configure the second peer site, if required.

i Click on the Properties button next to the Second Peer Site ID parameter in the MC IPsec panel. The MC IPsec (Edit) form opens with the General tab displayed.

ii Click on the Tunnel Groups tab.

iii Choose a tunnel group and click on the Properties button. The MC IPsec Tunnel Group (Edit) form opens with the General tab displayed.

iv Set the Administrative State parameter to Down.

v Click on the OK button. A dialog box appears.

vi Click on the Yes button. The MC IPsec Tunnel Group (Edit) form closes.

vii Repeat steps iii to vi to set the Administrative State parameter to Down for additional tunnel groups, if required.

viii Click on the General tab.

ix Configure the parameters:

- Keep-Alive Interval (deciseconds)
- Lost Connection Wait Multiplier
- Discovery Interval (seconds)
- Post-Boot Discovery Interval (seconds)
- Enable BFD

x Click on the OK button. A dialog box appears.

xi Click on the Yes button. The MC IPsec (Edit) form closes.

7 Close the MC Peer Group (Edit) form.

8 Close the Manage Node Redundancy form.

38 — MC endpoint groups

38.1 MC endpoint groups overview *38-2*

38.2 Workflow to manage MC endpoint groups *38-2*

38.3 MC endpoint groups management procedures *38-3*

38.1 MC endpoint groups overview

An MC endpoint group consists of two MC endpoint peers that are configured as peers in a pair of sites. Multiple VPLS endpoints can use the MC endpoint peer. The endpoints must be on a 7450 ESS, 7710 SR, 7750 SR, or 7950 XRS, and must support PW redundancy. Each endpoint can be associated with different destinations, with a maximum of two spoke SDPs for each endpoint. The endpoints communicate with each other to get the associated status of the spoke SDPs, which ensures that only one spoke SDP is active at any time; the other spoke SDPs have a standby status. The grouping of multiple spoke SDPs that are associated with the two MC endpoint peers eliminates traffic loops in a VPLS or B-VPLS.

An MC endpoint group includes:

- two MC endpoint peers that can be used by a spoke SDP, which is under mc-endpoint and relies on mc-ep-peer in the CLI
- an MC protocol that is used for:
  - determination of which MC endpoint peers are active or standby
  - synchronization of the pseudo-wire information that is between the MC endpoint peers
  - fault detection using centralized BFD. The MC endpoint protocol contains a keep-alive mechanism because BFD cannot detect whether an MC endpoint peer is shut down or if there is a configuration problem.
- T-LDP signaling, which is used to communicate whether the pseudo-wire is active or standby to other gateway pairs. The other gateway pairs may not have an MC endpoint.

An MC peer group that is managed by the 5620 SAM contains two MC peers. Each MC peer is configured as the peer of the other MC peer. An MC peer group must be created before you create an MC endpoint group. When only one peer in an MC peer group is managed by the 5620 SAM, you can configure node redundancy parameters only for the managed peer and only from the NE properties form. See chapter 36 for more information about MC peer groups.

BFD

The MC endpoint protocol uses the keep-alive mechanisms. The MC endpoint protocol also supports BFD to eliminate traffic loops. See Procedure 38-1 for information about how to configure an MC endpoint group for BFD.

38.2 Workflow to manage MC endpoint groups

1. Create an MC peer group, as described in chapter 36.
2. Create an MC endpoint group. See Procedure 38-1 for more information.
3. Create and configure the VPLS. See chapter 68 for more information.
4. As required, create an MC LAG group. See chapter 39 for more information.

5 As required, create an MC synchronization group. See chapter 40 for more information.

6 As required, create an MC ring group. See chapter 41 for more information.

38.3 MC endpoint groups management procedures

Use the following procedures to perform MC endpoint group management tasks.

Procedure 38-1 To configure an MC endpoint group

1 Create an MC peer group, as described in Procedure 36-1.

2 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

3 Choose MC Peer Group (Multi-Chassis) from the object drop-down list.

4 Configure the filter criteria and click on the Search button. A list of MC peer groups is displayed.

5 Select an MC peer group and click on the Properties button. The MC Peer Group (Edit) form opens with the General tab displayed.

6 Click on the Associated Groups tab.

7 Right-click on MC Endpoint Group and choose Create MC Endpoint Group from the contextual menu. The MC Endpoint Group (Create) form opens.

8 Configure the Description parameter.

9 Configure the parameters for the MC Endpoint on First Site:

- System Priority
- Keep-Alive Interval (deciseconds)
- Hold On Neighbor Failure
- Administrative State
- Passive Mode Enabled
- BFD Enabled
- Boot Timer

10 Configure the parameters for the MC Endpoint on Second Site:

- System Priority
- Keep-Alive Interval (deciseconds)
- Hold On Neighbor Failure
- Administrative State
- Passive Mode Enabled
- BFD Enabled
- Boot Timer

11 Click on the OK button.

12 Close the MC Peer Group (Edit) form.

13 Close the Manage Node Redundancy form.

14 Create a VPLS, site, and VPLS endpoint, as described in Procedure 68-1 and Procedure 68-15.



Note — In Procedure 68-1, set the Endpoint Type parameter to Multi Chassis.

15 Click on the Yes button.

16 Perform one of the following:

a Create a redundant spoke SDP binding under an endpoint, as described in steps 4 to 40 of Procedure 68-44.

b Create a spoke SDP binding for the site, as described in steps 9 to 40 of Procedure 68-44.

Procedure 38-2 To modify an MC endpoint group

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Endpoint Group (Multi-Chassis) from the Select Object Type drop-down list.

3 Configure the filter criteria and click on the Search button. A list of MC endpoint groups is displayed.

4 Choose an MC endpoint group and click on the Properties button. The MC Endpoint Group (Edit) form opens with the General tab displayed.

5 Configure the Description parameter.

6 Configure the parameters for the MC Endpoint on First Site:

- System Priority
- Keep-Alive Interval (deciseconds)
- Hold On Neighbor Failure
- Administrative State
- Passive Mode Enabled
- BFD Enabled
- Boot Timer

7 Configure the parameters for the MC Endpoint on Second Site:

- System Priority
- Keep-Alive Interval (deciseconds)
- Hold On Neighbor Failure
- Administrative State
- Passive Mode Enabled
- BFD Enabled
- Boot Timer

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button. The MC Endpoint Group form closes.

Procedure 38-3 To view an MC endpoint peer on one NE

Perform this procedure to view an MC endpoint peer when only one NE in the MC endpoint group is managed by the 5620 SAM.



Note — This procedure assumes that you have already configured an MC peer group with an associated MC endpoint group. If only one NE is managed by the 5620 SAM, you must create these objects from the CLI.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the NE where you want to view an MC endpoint peer and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Redundancy tab.

4 Click on the MC Peer tab.

5 Configure the filter criteria, if required, and click on the Search button.

6 Choose an MC Peer in the list and click on the Properties button. The MC Peer (Edit) form opens with the General tab displayed.

7 Click on the MC Endpoint tab.

8 Configure the filter criteria, if required, and click on the Search button.

9 Choose an MC endpoint peer in the list and click on the Properties button. The MC Endpoint (Edit) form opens with the General tab displayed.

10 View the information, as required.

11 Close the MC Endpoint (Edit) form.

12 Close the MC Peer (Edit) form.

13 Close the Network Element (Edit) form.

Procedure 38-4 To delete an MC endpoint group



Caution — When you perform this procedure, the MC endpoint group is deleted from the 5620 SAM and member NE configurations. In addition, deleting an MC endpoint group removes all of the MC configurations that are associated with the MC peer group.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Endpoint Group (Multi-Chassis) from the object list.

3 Configure the filter criteria and click on the Search button. A list of MC endpoint groups is displayed.

4 Choose one or more MC endpoint groups in the list and click on the Delete button. A dialog box appears.

5 Click on the View Dependencies button. A warning form opens.

6 View the dependency information.

7 Select the I understand the implications of this action check box.

8 Click on the Yes button. The 5620 SAM deletes the MC endpoint group and the corresponding configuration for each member site.

If there are MC endpoints that use the MC endpoint group, you cannot delete the MC endpoint group. Remove the MC endpoints from the MC endpoint group and repeat steps 1 to 9.

9 Close the Manage Node Redundancy form.

39 — MC LAG groups

39.1 MC LAG groups overview *39-2*

39.2 Workflow to manage MC LAG groups *39-2*

39.3 MC LAG groups management procedures *39-3*

39.4 MC AOS groups overview *39-7*

39.5 Workflow to manage MC AOS groups *39-8*

39.6 MC AOS groups management procedures *39-8*

39.1 MC LAG groups overview

A LAG is a group of physical ports that form one logical link between two NEs to increase bandwidth, allow load balancing, and provide seamless redundancy. LAG support over multiple devices provides node-level redundancy in addition to link-layer redundancy using a switchover function. An MC LAG configuration provides redundant L2 access connectivity that extends beyond link-layer protection by allowing two devices to share a common LAG end point.

An MC LAG configuration includes one active member NE and one standby member NE. The active and standby NEs synchronize the link state information to facilitate link-layer messaging between an access node and each NE. This active and standby NE coupling provides a synchronized forwarding plane to and from the access node. LACP is used to manage the active and standby states of the available LAG links; only the links of one member NE at a time are active.

The 7450 ESS, 7710 SR, 7750 SR, and 7950 XRS support the creation of MC LAG groups using Ethernet ports in Access mode.

The OS 6900 and OS 10K (Release 7.3.1 or later) support the creation of MC AOS groups and MC AOS LAG groups.

The 7705 SAR-8, 7705 SAR-18, 7705 SAR-A, 7705 SAR-M and 7705 SAR-W support the creation of MC LAG groups to provide redundancy at the node level. The operator has the option of creating an alternative path for deploying a service on these redundant nodes. The 7705 SAR-8, 7705 SAR-18, 7705 SAR-A, 7705 SAR-M and 7705 SAR-W support inter-chassis backup (ICB) on MC LAG in order to provide redundant paths for the Epipe service.

When you use the 5620 SAM to change the MC LAG configuration on an NE, the 5620 SAM automatically updates the MC LAG configuration on the other NE. When you change the MC LAG configuration on an NE using, for example, a CLI, the 5620 SAM detects the configuration mismatch between the NEs and raises an alarm. The alarm information includes the type of configuration mismatch.

You can create an MC LAG group only from within an existing MC peer group. When only one peer in an MC peer group is managed by the 5620 SAM, you can configure node redundancy parameters only for the managed peer and only from the NE properties form. See chapter 36 for more information about MC peer groups.

MC synchronization

When subscriber management is enabled on an NE in an MC LAG configuration, the NE maintains dynamic state information for each subscriber host. The active and standby NEs synchronize this information to ensure uninterrupted service delivery in the case of an MC LAG switchover.

See chapter 40 for more information about MC synchronization.

39.2 Workflow to manage MC LAG groups

1. Create one or more LAGs using Ethernet access ports, as required. See chapter 14 for more information.
2. Create an MC peer group. See chapter 36 for more information.

3 Create an MC LAG group. See Procedure 39-1 for more information.

4 As required, configure MC LAG group members. See Procedure 39-2 for more information.

5 As required, configure MC LAG peer on one NE. See Procedure 39-3 for more information.

39.3 MC LAG groups management procedures

Use the following procedures to perform MC LAG management tasks.

Procedure 39-1 To create an MC LAG group

Perform this procedure to create an MC LAG group or to modify an existing MC LAG group. Consider the following before you create an MC LAG group:

- You can create an MC LAG member only on an Ethernet MDA.
- MC LAG member ports must be in Access mode.
- The 5620 SAM assigns the same LACP key, system ID, and system priority to each MC LAG member.
- MC LAGs are not supported when MAC subnetting is enabled.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Peer Group (Multi-Chassis) from the object drop-down list.

3 Click on the Search button. A list of MC peer groups is displayed.

4 Select an MC peer group in the list and click on the Properties button. The MC Peer Group (Edit) form opens.

5 Click on the Associated Groups tab.

6 Right-click on the MC Lag object in the navigation tree and choose Create MC LAG Group. The MC LAG Group (Create) form opens.

7 Configure the parameters:

- LACP Key
- System ID
- System Priority
- Description

8 Configure the PBB Source Backbone MAC LSB parameters:

- Use LACP Key
- MAC LSB (hex)



Note 1 — The parameters are only configurable on the 7750 SR, 7750 SR-c12, 7750 SR-12E, 7450 ESS, and 7950 XRS. The NE must also be configured with an IOM 3 MDA or an XMA.

Note 2 — An MC LAG has two members. The parameters can be configured only when both peers are PBB-capable; for example, if the peers are either the 7750 SR, 7750 SR-c12, 7750 SR-12E, 7450 ESS, or 7950 XRS. If both peers are PBB-incapable, the PBB parameters are not displayed.

9 Perform the following steps to choose the LAG for the first MC LAG member.

i Click on the Select button beside the LAG ID parameter in the First Site panel. The Select LAG form opens.

ii If no LAGs are listed, you can create a LAG by clicking on the Create button and performing steps 5 to 24 of Procedure 14-10.

iii Select a LAG in the list and click on the OK button. The Select LAG form closes and the MC LAG (Create) form displays the LAG information.

10 Perform the following steps to choose the LAG for the first MC LAG member.



Note — If you are configuring access dual-homing with local switching over PBB tunnels, the L2 access interfaces must be on LAGs that participate in the MC LAG. See Procedure 67-27 to configure L2 access interfaces.

i Click on the Select button beside the LAG ID parameter in the Second Site panel. The Select LAG form opens.

ii If no LAGs appear in the list, you can create a LAG by clicking on the Create button and performing steps 5 to 24 of Procedure 14-10.

iii Select a LAG in the list and click on the OK button. The Select LAG form closes and the MC LAG (Create) form displays the LAG information.

11 Click on the OK button. The MC LAG (Create) form closes, and the new MC LAG object is displayed below the MC LAG object in the navigation tree on the MC Peer Group (Edit) form.

12 Close the MC Peer Group (Edit) form.

13 Close the Manage Node Redundancy form.

Procedure 39-2 To configure an MC LAG group member

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC LAG Group (Multi-Chassis) from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of MC LAGs is displayed.

4 Select an MC LAG in the list and click on the Properties button. The MC LAG Group (Edit) form opens with the General tab displayed.

5 Configure the MC LAG parameters that are common to each member, if required:

- LACP Key
- System ID
- System Priority
- Description

6 Click on the States tab.

7 Click on the Properties button beside the Administrative State field in the MC Peer Communication section of the First Site panel. The MC Peer (Edit) form opens with the General tab displayed.

8 Configure the MC LAG member by performing the following steps.

i Click on the MC LAG tab. The General tab is displayed.

ii Configure the parameters:

- Keep-Alive Interval (deciseconds)
- Lost Connection Wait Interval
- Administrative State

iii Click on the OK button. A dialog box appears.

iv Click on the Yes button. The MC Peer (Edit) form closes.

9 Click on the Properties button beside the Administrative State field in the MC Peer Communication section of the Second Site panel. The NE Synchronization (Edit) form opens with the General tab displayed.

10 Repeat step 8.

11 Close the MC LAG Group (Edit) form.

12 Close the Manage Node Redundancy form.

Procedure 39-3 To configure an MC LAG peer on one NE

Perform this procedure to configure an MC LAG peer when only one NE in the MC LAG group is managed by the 5620 SAM.



Note — This procedure assumes that you have already configured an MC peer group with an associated MC LAG group. If only one NE is managed by the 5620 SAM, you must create these objects from the CLI.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the NE where you want to configure an MC LAG peer and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Redundancy tab.

4 Click on the MC Peer tab.

5 Configure the filter criteria, if required, and click on the Search button.

6 Choose an MC Peer in the list and click on the Properties button. The MC Peer (Edit) form opens with the General tab displayed.

7 Click on the MC LAG tab.

8 Configure the parameters:

- Keep-Alive Interval (deciseconds)
- Lost Connection Wait Interval
- Administrative State

9 Click on the Members tab.

10 Configure the filter criteria, if required, and click on the Search button.

11 Choose a member in the list and click on the Properties button. The MC LAG (Edit) form opens with the General tab displayed.

12 View the information, as required.

13 Close the MC LAG (Edit) form.

14 Close the MC Peer (Edit) form.

15 Close the Network Element (Edit) form.

Procedure 39-4 To delete an MC LAG group

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC LAG Group (Multi-Chassis) from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of MC LAG groups is displayed.

4 Select one or more MC LAG groups in the list and click on the Delete button. A dialog box appears.

5 Click on the View Dependencies button. An information dialog box appears.

6 View the dependency information.

7 Click on the OK button.

8 Click on the Yes button. The 5620 SAM deletes the MC LAG group and the corresponding configuration on each member site.



Note — If you change the default values of the Keep-Alive Interval (deciseconds) and Lost Connection Wait Interval parameters in step 8ii of Procedure 39-2, the MC LAG group configuration of the member sites is not removed. You can view the MC LAG member information under the LAG icon in the network view of the navigation tree.

9 Close the Manage Node Redundancy form.

39.4 MC AOS groups overview

MC AOS groups enable the creation of MC LAGs on OS 9700E and OS 9800E, Release 6.4.5 or later (XNI-U12E cards only), as well as OS 6900 and OS 10K, Release 7.3.1 or later. This functionality is supported on the node side from 7.2.1. Configured MC LAGs should be removed from any 7.2.1 OS 6900 or OS 10K before being discovered by the 5620 SAM. Similarly, any 7.3.1 OS 6900 or OS 10K with configured MC LAGs that is downgraded to 7.2.1 will cause an object not found exception.



Warning — When MC LAGs are configured on any of the above NEs, Ethernet OAM and SAA configurations should not be attempted.

An MC LAG configuration includes one active member NE and one standby member NE. The active and standby NEs synchronize the link state information to facilitate link-layer messaging between an access node and each NE. This active and standby NE coupling provides a synchronized forwarding plane to and from the access node. LACP is used to manage the active and standby states of the available LAG links; only the links of one member NE at a time are active.

39.5 Workflow to manage MC AOS groups

1. Create one or more LAGs using OmniSwitch ports, as required. See chapter 14 for more information.
2. Create an MC AOS Group. See Procedure 39-5 for more information.
3. Create an MC AOS VFLink group. See Procedure 39-6 for more information.
4. Create an MC AOS LAG Group. See Procedure 39-7 for more information.
5. As required, configure MC AOS Group members. See Procedure 39-8 for more information.

39.6 MC AOS groups management procedures

Use the following procedures to perform MC AOS management tasks.

Procedure 39-5 To create an MC AOS group

Perform this procedure to create an MC AOS group or to modify an existing MC AOS group.

1. Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.
2. Choose MC AOS Group (Aos Redundancy) from the object drop-down list.
3. Click on the Create button. The MC AOS Group (Create) form opens with the General tab displayed.
4. Configure the parameters:
   - Chassis Group
   - Auto-Assign ID
   - Hello Interval (seconds)
5. Perform one of the following:
   a. Configure the parameters in the First MultiChassis (Chassis Id 1) panel:
      - Chassis ID
      - Chassis Group
      - Hello Interval (seconds)
   b. Select an OmniSwitch multichassis:
      i. Click on the Select button in the First MultiChassis (Chassis Id 1) panel. A list of OmniSwitch multichassis appears.
      ii. Choose an OmniSwitch multichassis from the list and click on the OK button. The MC AOS Group (Create) form reappears with the first multichassis information displayed.

6 Perform one of the following:

a Configure the parameters in the Second MultiChassis (Chassis Id 2) panel:

- Chassis ID
- Chassis Group
- Hello Interval (seconds)

b Select an OmniSwitch multichassis:

i Click on the Select button in the Second MultiChassis (Chassis Id 2) panel. A list of OmniSwitch multichassis appears.

ii Choose an OmniSwitch multichassis from the list and click on the OK button. The MC AOS Group (Create) form reappears with the second multichassis information displayed.

7 Perform one of the following:

a Configure the IPC VLAN Site ID parameter.

b Enable the Default parameter.

8 Configure the parameters:

- Configure Primary Lag Range
- Primary Minimum Lag Id
- Primary Maximum Lag Id
- Configure Seconday Lag Range
- Secondary Minimum Lag Id
- Secondary Maximum Lag Id
- Configure MultiChassis Lag Range
- Minimum MCLag Id
- Maximum MCLag Id

The Primary Minimum Lag Id and Primary Maximum Lag Id parameters are only configurable when the Configure Primary Lag Range parameter is enabled.

The Secondary Minimum Lag Id and Secondary Maximum Lag Id parameters are only configurable when the Configure Secondary Lag Range parameter is enabled.

The Minimum MCLag Id and Maximum MCLag Id parameters are only configurable when the Configure MultiChassis Lag Range parameter is enabled.

9 Right-click on MC AOS LAG Group and choose Create MC AOS LAG Group from the contextual menu. The MC AOS LAG Group (Create) form opens.

10 Configure the Lag ID parameter.

11 Click on the OK button. A dialog box appears.

12 Click on the OK button. The MC AOS LAG Group (Create) form closes.

13 Click on the OK button. The MC AOS Group (Create) form closes.

Procedure 39-6 To create an MC AOS VFLink Group

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC AOS Group (Aos Redundancy) from the object drop-down list.

3 Click on the Search button. A list of MC AOS Groups is displayed.

4 Choose an MC AOS Group from the list and click on the Properties button. The MC AOS Group (Edit) form opens.

5 Click on the Associated Groups tab.

6 Right-click on MC AOS VFLink Group and choose Create MC AOS VFLink Group from the contextual menu. The AOS VFLink Group (Create) form opens.

7 Click on the Select button in the Default Vlan for VFLink panel. The Select Default Vlan for VFLink form opens with a list of VLANs displayed.

8 Select a VLAN from the list and click on the OK button. The Select Default Vlan for VFLink form closes and the AOS VFLink Group (Create) form reappears with the VLAN information displayed.

9 Click on the Apply button.

10 Click on the Properties button in the First MultiChassis VFLinkEnd (Chassis Id 1) panel. The AOS VF Link End form opens with the General tab displayed.

11 Click on the VF Link End Member Port tab.

12 Click on the Create button. The Select Port - AOS VF Link End form opens with a list of ports displayed.



Note — A maximum of 8 member ports can be added for each multichassis. These must be access ports with a speed of 10-Gig or above.

13 Choose a port from the list and click on the OK button. The Select Port - AOS VF Link End form closes and the AOS VF Link End form reappears with the port information displayed.

14 Repeat steps 12 and 13 to add additionational member ports to the first chassis.

15 Click on the Properties button in the Second MultiChassis VFLinkEnd (Chassis Id 2) panel. The AOS VF Link End form opens with the General tab displayed.

16 Click on the VF Link End Member Port tab.

17 Click on the Create button. The Select Port - AOS VF Link End form opens with a list of ports displayed.

18 Choose a port from the list and click on the OK button. The Select Port - AOS VF Link End form closes and the AOS VF Link End form reappears with the port information displayed.



Note — This member port cannot be used as a learned port security, VLAN access interface, or LAG member. Attempting to use the member port in these ways will cause deployment failures.

19 Repeat steps 15 to 18 to add additionational member ports to the second chassis.

20 Click on the OK button. The AOS VF Link End form closes.

21 Click on the OK button. The AOS VFLink Group (Edit) form closes.

22 Click on the OK button. The MC AOS Group (Edit) form closes.

Procedure 39-7 To create an MC AOS LAG Group

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC AOS Group (Aos Redundancy) from the object drop-down list.

3 Click on the Search button. A list of MC AOS Groups is displayed.

4 Choose an MC AOS Group from the list and click on the Properties button. The MC AOS Group (Edit) form opens.

5 Click on the Associated Groups tab.

6 Right-click on MC AOS LAG Group and choose Create MC AOS LAG Group from the contextual menu. The MC AOS LAG Group (Create) form opens.

7 Configure the Lag ID parameter.



Note — Configuring the Lag ID parameter with a range of Peer or MultiChassis will result in a deployment failure.

8 Click on the OK button. A dialog box appears.

9 Click on the OK button. The MC AOS LAG Group (Create) form closes.

10 Click on the OK button. The MC AOS Group (Edit) form closes.

Procedure 39-8 To configure an MC AOS group member

1 Right-click on an applicable OmniSwitch NE in the navigation tree and choose Properties from the contextual menu. The NE properties form opens.

2 Click on the MultiChassis tab.

3 Configure the parameters:

- Chassis ID
- Chassis Group
- Hello Interval (Seconds)
- IPC VLAN

4 Click on the Lag Ranges tab.

5 Configure the parameters:

- Configure Local Lag Range
- Local Minimum Lag ID
- Local Maximum Lag ID
- Configure Peer Lag Range
- Peer Minimum Lag ID
- Peer Maximum Lag ID
- Configure Local Lag Range
- Minimum MCLag ID
- Maximum MCLag ID

The Local Minimum Lag ID and Local Maximum Lag ID parameters are only configurable when the Configure Local Lag Range parameter is enabled.

The Peer Minimum Lag ID and Peer Maximum Lag ID parameters are only configurable when the Configure Peer Lag Range parameter is enabled.

The Minimum MCLag ID and Maximum MCLag ID parameters are only configurable when the Configure Local Lag Range parameter is enabled.

6 Click on the Loopback Detection tab.

7 Configure the Admin Status and Transmit Interval (seconds) parameters.

8 Click on the OK button. The NE properties form closes.

40 — MC synchronization groups

40.1 MC synchronization groups overview *40-2*

40.2 Workflow to manage MC synchronization groups *40-3*

40.3 MC synchronization groups management procedures *40-3*

40.1 MC synchronization groups overview

When subscriber management is enabled on an NE, the NE maintains dynamic subscriber-host state information. The state information must be synchronized between the active and standby NEs in a redundant configuration to ensure that service delivery is uninterrupted if a switchover occurs.

The 7210 SAS-M, 7210 SAS-X, 7450 ESS, 7710 SR, 7750 SR, and 7950 XRS support the creation of MC synchronization groups using Ethernet ports in Access mode.



Note — You can create an MC synchronization group only from within an existing MC peer group. See chapter 36 for more information about MC peer groups.

MC synchronization can be used to ensure that the following dynamic state information is synchronized:

- Basic and enhanced subscriber management
- IGMP snooping in VPLS
- IGMP on IES or VPRN group interfaces
- SRRP in VPRN

You create an MC synchronization group inside an MC peer group using a unique synchronization tag to define the pair of NEs and the two ports or LAGs on which the dynamic state information is synchronized. The synchronization is applied to all SAPs on the port or LAG that have the same synchronization tag. When only one peer in an MC peer group is managed by the 5620 SAM, you can configure node redundancy parameters only for the managed peer and only from the NE properties form. See chapter 36 for more information about MC peer groups.

A synchronization tag can be applied to a specified VLAN range on a port or LAG. All of the SAPs in the VLAN range are assigned the synchronization tag. The SAPs that are not in the VLAN range are not synchronized.



Note 1 — Only ports and LAGs that use dot1q or QinQ encapsulation support MC synchronization.

Note 2 — MC synchronization group VLAN ranges are configurable only after MC synchronization group creation.

Note 3 — If the 5620 SAM detects a port or VLAN range configuration mismatch in an MC synchronization group during NE discovery, the 5620 SAM raises an alarm.

MC synchronization and dual-homed L2/L3 CO

MC synchronization is typically used in a dual-homed L2 or L3 CO configuration. For example, an access node that aggregates several subscriber lines can be dual-homed to a redundant pair of NEs. Dynamic subscriber-host state information on the NE must be synchronized with the redundant peer to ensure that service delivery in unaffected if a switchover occurs. See chapters 70 and 71 for more information about L2 and L3 CO dual homing.

MC synchronization for dual homing requires the configuration of protocol synchronization on the MC peer group that defines the redundant pair of NEs. See Procedure 36-1 for more information about configuring protocol synchronization on an MC peer group.

40.2 Workflow to manage MC synchronization groups

1 Create an MC peer group. See chapter 36 for information about MC peer groups.

2 Create an MC synchronization group, including MC peer synchronization ports or VLAN ranges. See Procedure 40-1 for more information.

3 Configure protocol synchronization for the MC synchronization group. See Procedure 40-2 for more information.

40.3 MC synchronization groups management procedures

Use the following procedures to perform MC synchronization management tasks.

Procedure 40-1 To create an MC synchronization group

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Peer Group (Multi-Chassis) from the object drop-down list and click on the Search button. A list of MC peer groups is displayed.

3 Select an MC peer group in the list and click on the Properties button. The MC Peer Group (Edit) form opens with the General tab displayed.

4 Click on the Associated Groups tab.

5 Right-click on the MC Sync Group object in the navigation tree and choose Create MC Sync Group from the drop-down menu. The MC Sync Group (Create) form opens.

6 Configure the parameters:

- Synchronization Tag
- Description
- Sync Tag Config Level

7 Specify the port, PW port, or LAG on the first NE.

Click on the Select button beside the Port/LAG Name parameter in the First Element panel. The Select Port/LAG - MC Sync Group form opens.



Note — If you set the Sync Tag Config Level parameter to VLAN Range Level, only dot1q and QinQ-encapsulated Ethernet ports, PW ports, or LAGs in Access mode are listed.

8 Select a port, PW port, or LAG in the list and click on the OK button. The Select Port/LAG - MC Sync Group form closes, and the port or LAG information is displayed on the MC Sync Group (Create) form.

9 Specify the port or LAG on the second NE.

Click on the Select button beside the Port/LAG Name parameter in the Second Element panel. The Select Port/LAG - MC Sync Group form opens.



Note — Only ports or LAGs that have the same encapsulation type as the port or LAG on the first NE are listed.

10 Select a port or LAG in the list and click on the OK button. The Select Port/LAG - MC Sync Group form closes, and the port or LAG information is displayed on the MC Sync Group (Create) form.

11 If you set the Sync Tag Config Level parameter to VLAN Range Level, perform the following steps to specify the VLAN ranges that the MC synchronization group is to monitor.



Note — The VLAN ranges that you configure are applied to the configuration of each site in the MC synchronization group.

i Click on the Apply button. The form displays additional tabs.

ii Click on the First Site VLAN Entries tab.

iii Click on the Create button. The VLAN Range (Create) form opens.

iv Configure the parameters:

- Minimum Outer Encap Value
- Maximum Outer Encap Value
- Minimum Inner Encap Value
- Maximum Inner Encap Value

The Minimum Inner Encap Value and Maximum Inner Encap Value parameters are configurable only when the encapsulation type of the associated ports or LAGs is QinQ.

v Click on the OK button. The VLAN Range (Create) form closes.

vi Repeat steps 11 iii to v to add another VLAN range, if required.

12 Close the MC Sync Group (Create) form.

13 Close the MC Peer Group (Edit) form.

14 Close the Manage Node Redundancy form.

Procedure 40-2 To configure protocol synchronization between MC peer group members

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Peer Group (Multi-Chassis) from the object drop-down list and click on the Search button. A list of MC peer groups is displayed.

3 Select an MC peer group in the list and click on the Properties button. The MC Peer Group (Edit) form opens with the General tab displayed.

4 Click on the Synchronize Protocols tab.

5 Configure the parameters:

- Sync Administrative State
- IGMP
- IGMP Snooping
- Subscriber Management
- SRRP
- MC Ring
- MLD Snooping
- MC Ring

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The MC Synchronization (Edit) form closes.

8 Close the Manage Node Redundancy form.

Procedure 40-3 To view an MC synchronization peer on one NE

Perform this procedure to view an MC synchronization peer when only one NE in the MC synchronization group is managed by the 5620 SAM.

Note — This procedure assumes that you have already configured an MC peer group with an associated MC synchronization group. If only one NE is managed by the 5620 SAM, you must create these objects from the CLI.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the NE where you want to view an MC synchronization peer and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Redundancy tab.

4 Click on the MC Peer tab.

5 Configure the filter criteria, if required, and click on the Search button.

6 Choose an MC Peer in the list and click on the Properties button. The MC Peer (Edit) form opens with the General tab displayed.

7 Click on the Synchronization Protocol tab.

8 Configure the filter criteria, if required, and click on the Search button.

9 Choose an MC synchronization peer in the list and click on the Properties button. The MC Sync (Edit) form opens with the General tab displayed.

10 View the information, as required.

11 Close the MC Sync (Edit).

12 Close the MC Peer (Edit) form.

13 Close the Network Element (Edit) form.

Procedure 40-4 To delete an MC synchronization group

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Sync Group (Multi-Chassis) from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of MC synchronization groups is displayed.

4 Select one or more MC synchronization groups in the list and click on the Delete button. A dialog box appears.



Caution — Deleting an MC synchronization group that is associated with an MC ring group disables the protocol synchronization between the member sites in the MC ring group.

5 Click on the Yes button. The 5620 SAM deletes the MC synchronization group and the corresponding configuration on each member site.

6 Close the Manage Node Redundancy form.

41 — MC ring groups

41.1 MC ring groups overview *41-2*

41.2 Workflow to manage MC ring groups *41-7*

41.3 MC ring groups management procedures *41-10*

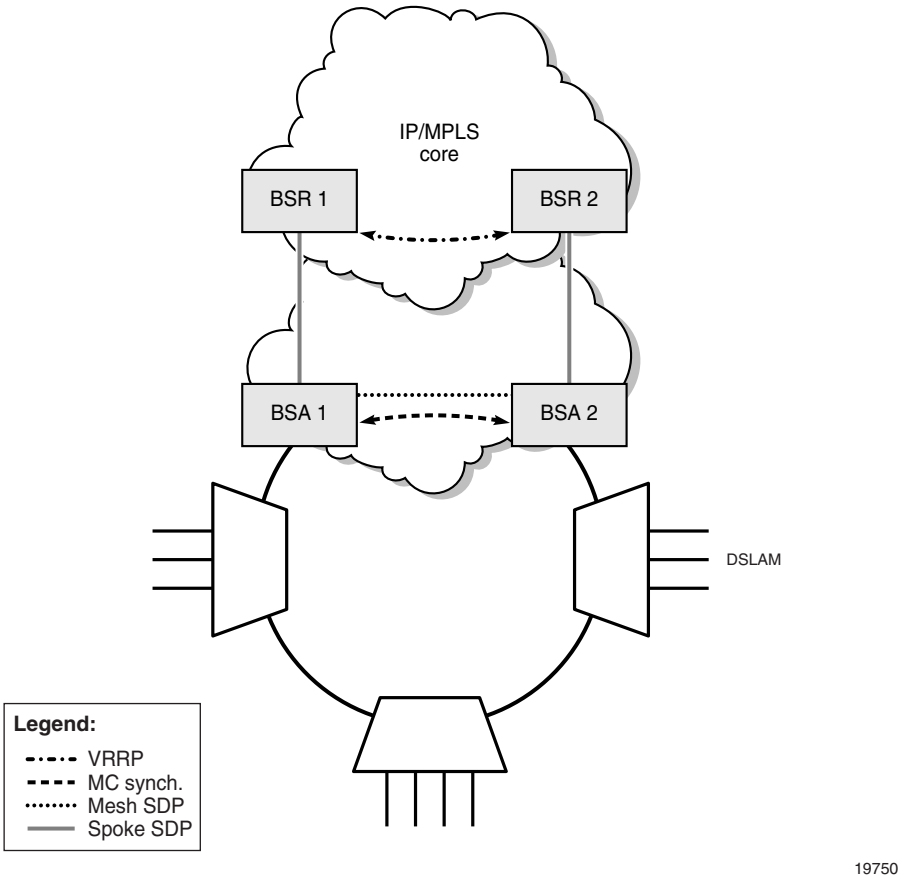
41.1 MC ring groups overview

5620 SAM MC ring groups are an extension of the dual-homing support available in TPSDA networks. MC ring groups provide aggregation redundancy in networks that have multiple access nodes, called ring nodes in the context of MC ring groups, connected in a single ring.

The 7210 SAS-M, 7450 ESS, 7710 SR, 7750 SR, and 7950 XRS support the creation of MC ring groups using Ethernet ports in Access mode.

Figure 41-1 shows a simple subscriber aggregation network in which a single ring of access nodes, such as DSLAMs, is connected to a BSA in a VPLS. Each BSA is connected to an IES or VPRN L3 interface on a BSR using a spoke SDP. Each BSR L3 interface aggregates the subscriber traffic in one subnet.

Figure 41-1 Simple subscriber aggregation network



Note 1 — BTV distribution is typically implemented in a separate VPLS that uses one SAP per access node.

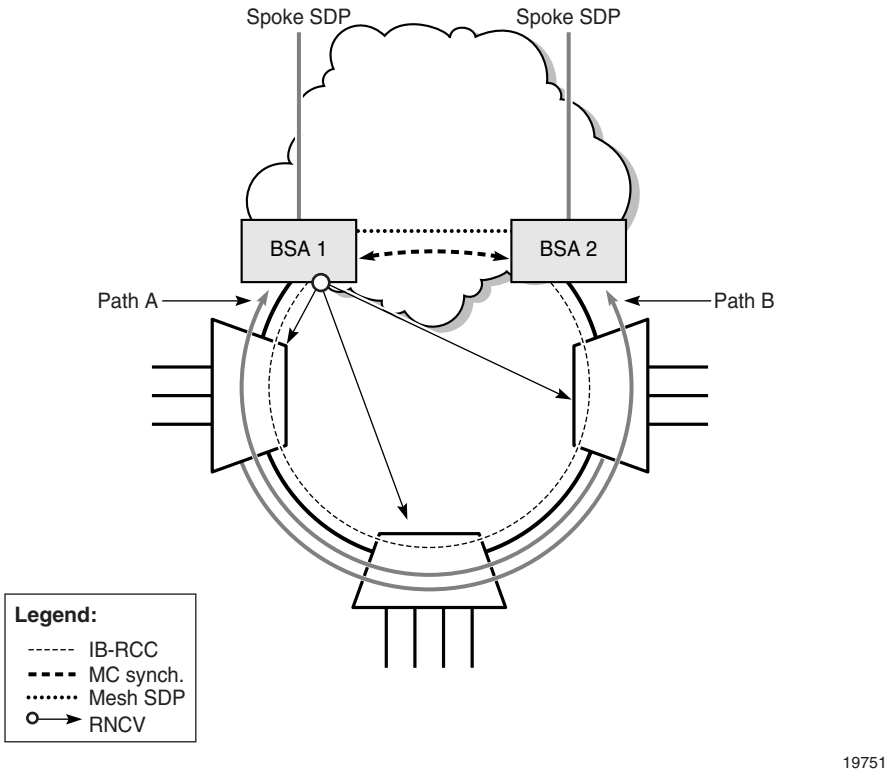
Note 2 — An MC ring group does not support a ring that has more than one break.

Steady-state condition

When an MC ring group is configured, the operation of a typical dual-homed ring is as shown in Figure 41-2. A steady-state condition is defined by the following.

- The participating BSAs have matching MC ring configurations.
- The In-Band Ring Control Connection, or IB-RCC, is operationally up.
- The MC ring is operationally up.

Figure 41-2 Dual-homed ring, steady-state condition



The IB-RCC is set up using a BFD session between IES or VPRN IP interfaces on BSA 1 and BSA 2. This connection requires a separate ring VLAN.

You can create an MC ring group only from within an existing MC peer group. When only one peer in an MC peer group is managed by the 5620 SAM, you can configure node redundancy parameters only for the managed peer and only from the NE properties form. See chapter 36 for more information about MC peer groups.

In the steady state, the ring is fully closed and each ring node has two paths to the VPLS core; these are shown as Path A and Path B. To prevent a communication loop, a ring node can use only one path for VLAN traffic. The VLAN range can be explicitly assigned to Path B on each BSA; by default, the SAP uses Path A. The VLAN range assignment for each path must be the same on each BSA. A SAP in the conflict range is assigned to Path A, regardless of the local configuration.

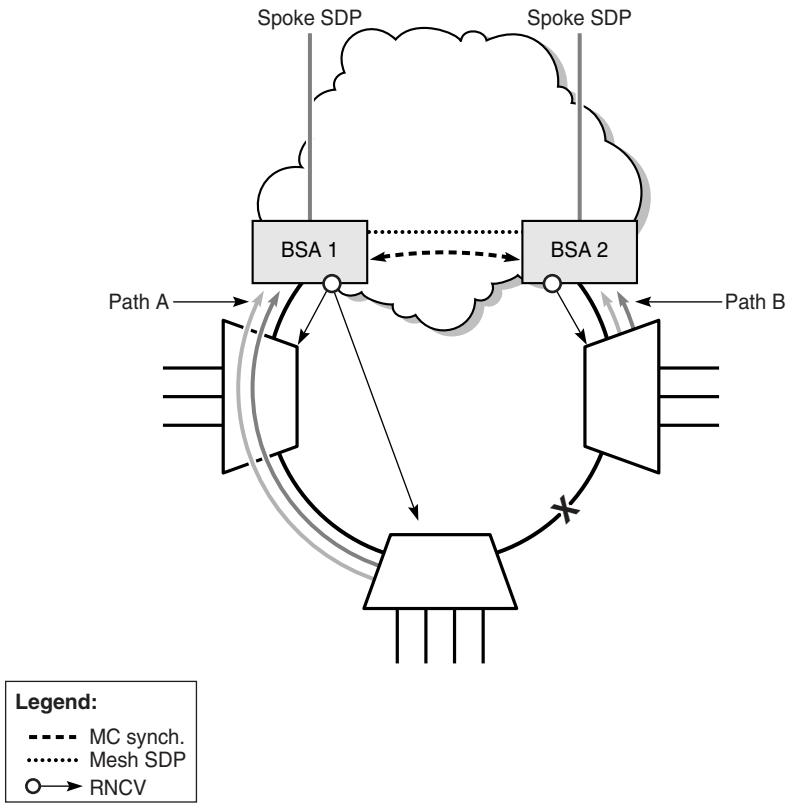
Each SAP in the path that ends on the master BSA is operationally up. Each subscriber-host forwarding database entry associated with the SAP points to the SAP. Each SAP in the path that ends on the standby BSA is operationally down. Each subscriber-host forwarding database entry associated with the SAP points to the mesh SDP that connects to the master BSA.

The master BSA periodically performs a Ring Node Connectivity Verification, or RNCV, check. The loss of connectivity to a ring node does not automatically trigger a switchover to the other path; if the IB-RCC BFD session is up, the ring is considered closed, and the master and standby BSA roles do not change.

Broken ring condition

A broken ring condition occurs when there is a link failure or ring node failure, as shown in Figure 41-3. In this condition, the IB-RCC is operationally down. Each ring node has only one path to the VPLS core.

Figure 41-3 Dual-homed ring, broken-ring condition



Each BSA becomes the master for the ring nodes that it can reach, and performs as described in the steady-state condition. Each L2 SAP on each BSA is operationally up, except the SAPs that are explicitly excluded from the MC ring control.

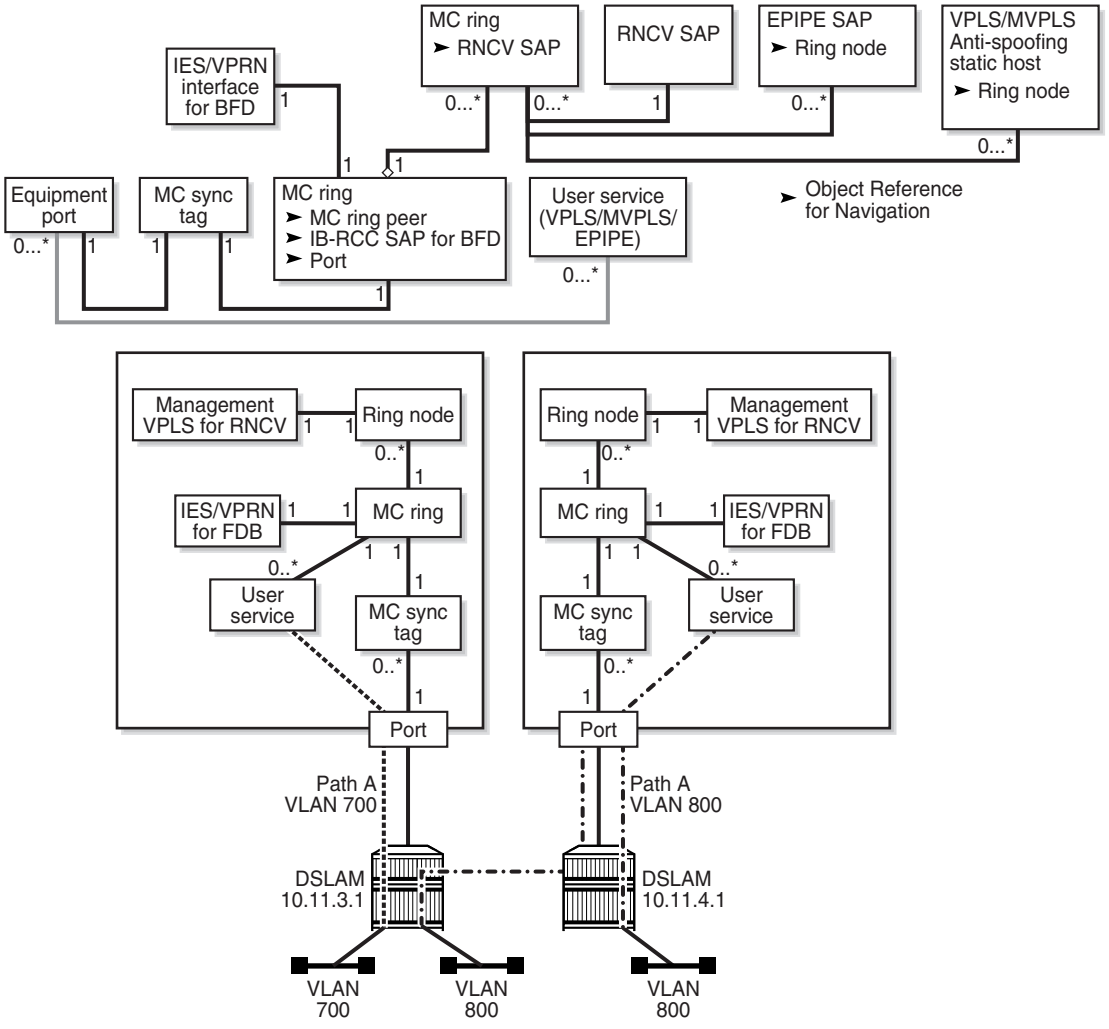
In the broken-ring condition, each BSA performs an RNCV check because each is a master. The forwarding database entry for each subscriber host behind a unreachable ring node points to the mesh SDP.

When the MC ring connectivity is restored, one BSA is the master for Path A and the other BSA is the master for Path B.

Object relationships

Figure 41-4 shows the MC ring and ring node object relationships with equipment and service objects.

Figure 41-4 MC ring group object relationships



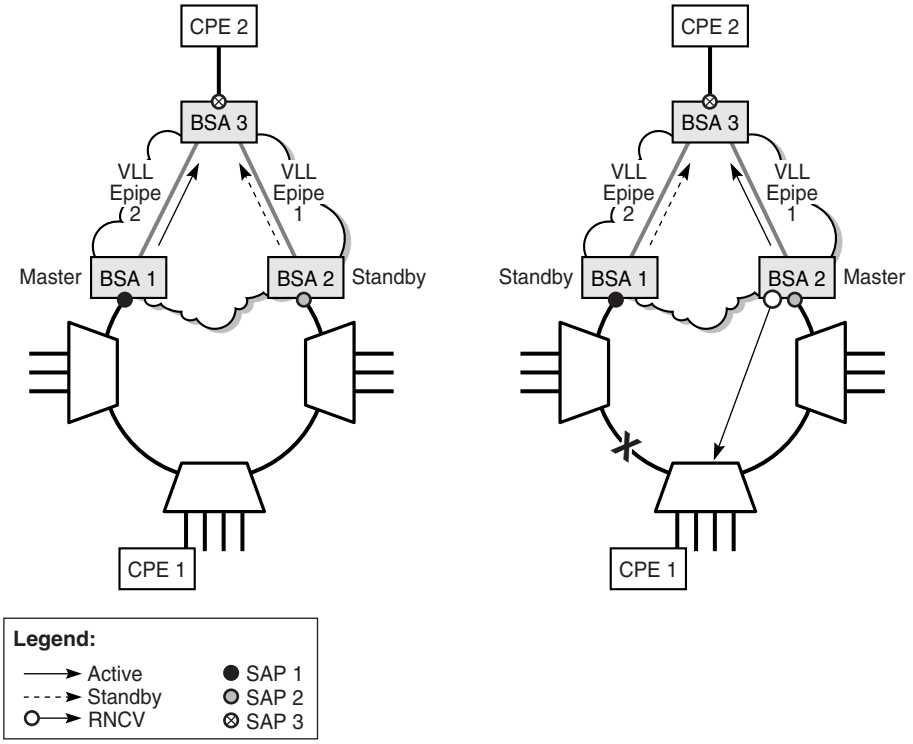
An MC ring has a one-to-one relationship with an MC synchronization tag. An MC ring uses one IES or VPRN service for IB-RCC. An MC ring can have multiple ring nodes, and each ring node can use only one SAP for RNCV.

When an MC ring group is correctly configured, each BSA L2 SAP is protected by the ring. The service that contains these protected SAPs is referred to as the user service. The service that is used for RNCV is an MVPLS that can also contain user SAPs and be a user service.

MC ring group and redundant VLL Epipe access operation

An MC ring group can connect to a VLL SAP to support redundant VLL Epipe access. Figure 41-5 shows a sample configuration using a VLL Epipe.

Figure 41-5 Dual-homed VLL Epipe configuration



CPE 1 connects to a ring node that has access to each BSA through a VLAN that is provisioned on each ring node. The SAP on each BSA uses the same VLAN tag.

In the closed ring on the left, BSA 1 is the master and sends an active status notification to BSA 3 on a VLL Epipe. BSA 2, the standby, sends a standby status notification. Based on this information, BSA 3 chooses a path to reach CPE 2.

In the broken ring on the right, the BSA that can use RNCV to reach CPE 1 becomes the master and sends an active status notification to BSA 3 on a VLL Epipe.

In each scenario, only one SAP is operationally up at a time, and each Epipe must be operationally up. If the ring node of CPE 1 is operationally down, neither BSA can reach the ring node, so each SAP and Epipe is operationally down.

MC ring groups and subscriber hosts

Each subscriber host on a SAP that is protected by an MC ring group must be associated with a ring node to determine whether the subscriber host is reachable by the BSA. Each VLL Epipe used for forwarding from an MC ring group must be explicitly configured with the name of a ring node in the MC ring. See Procedure 41-3 for information about configuring VLL Epipes for use with an MC ring group.

When subscriber management is enabled on a VPLS SAP, each dynamic subscriber host is automatically associated with a ring node. Static hosts on a VPLS SAP require explicit configuration. The following must be true before you can turn up an MC ring on a VPLS SAP that has one or more static hosts, or turn up a static host on a VPLS SAP in an operational MC ring:

- Subscriber management is enabled.
- The following are configured on the static host:
  - the name of a ring node in the MC ring group
  - subscriber identification
  - a subscriber profile
  - an SLA profile

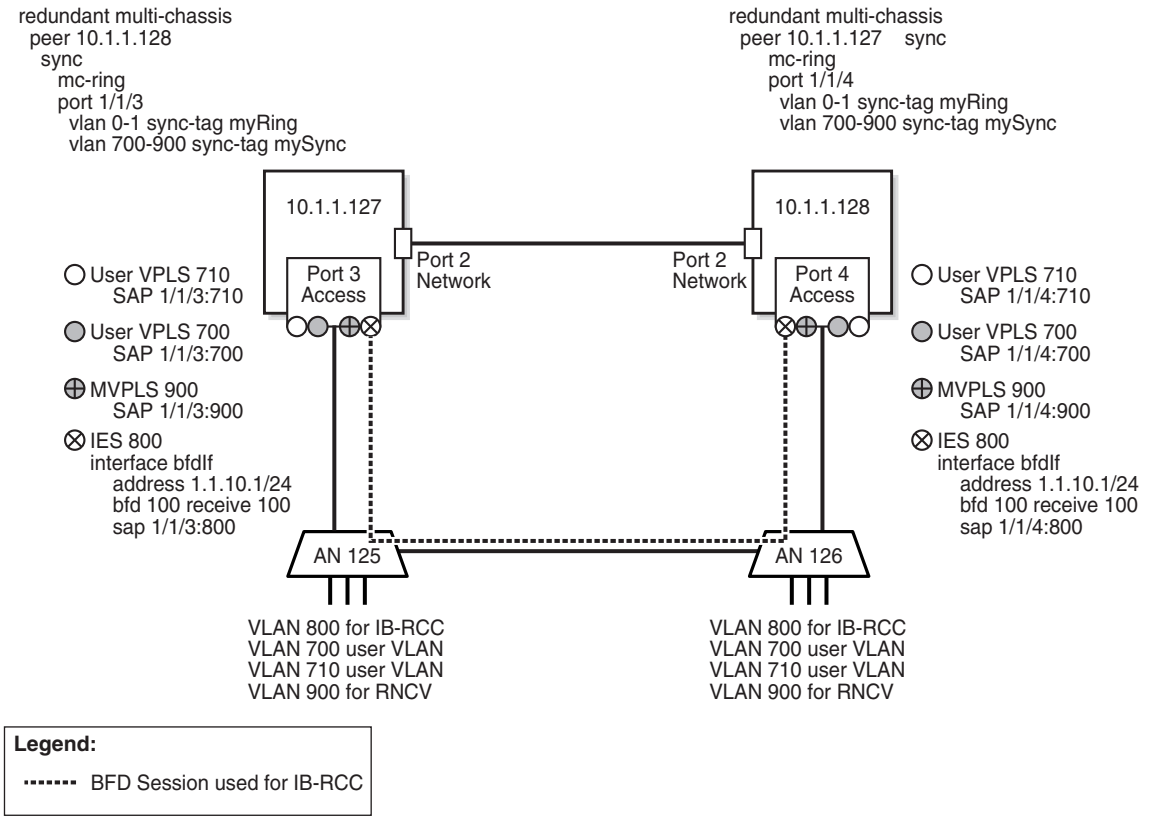
41.2 Workflow to manage MC ring groups

The following are the high-level steps required to perform MC ring group management.

NE preconfiguration

1 Configure physical connectivity between the two BSAs and the ring nodes, as shown in Figure 41-6. Each port must be operationally up.

Figure 41-6 MC ring group preconfiguration



19758

2 Configure a routing protocol on each BSA to enable IP communication. See chapter 23 for information about configuring routing protocols.

3 Configure an MVPLS for RNCV on the BSAs. See chapter 68 for information about configuring MVPLS.

4 Create an MC peer group that has the two BSAs as members and has MC ring synchronization enabled. See chapter 36 for information about MC peer groups.

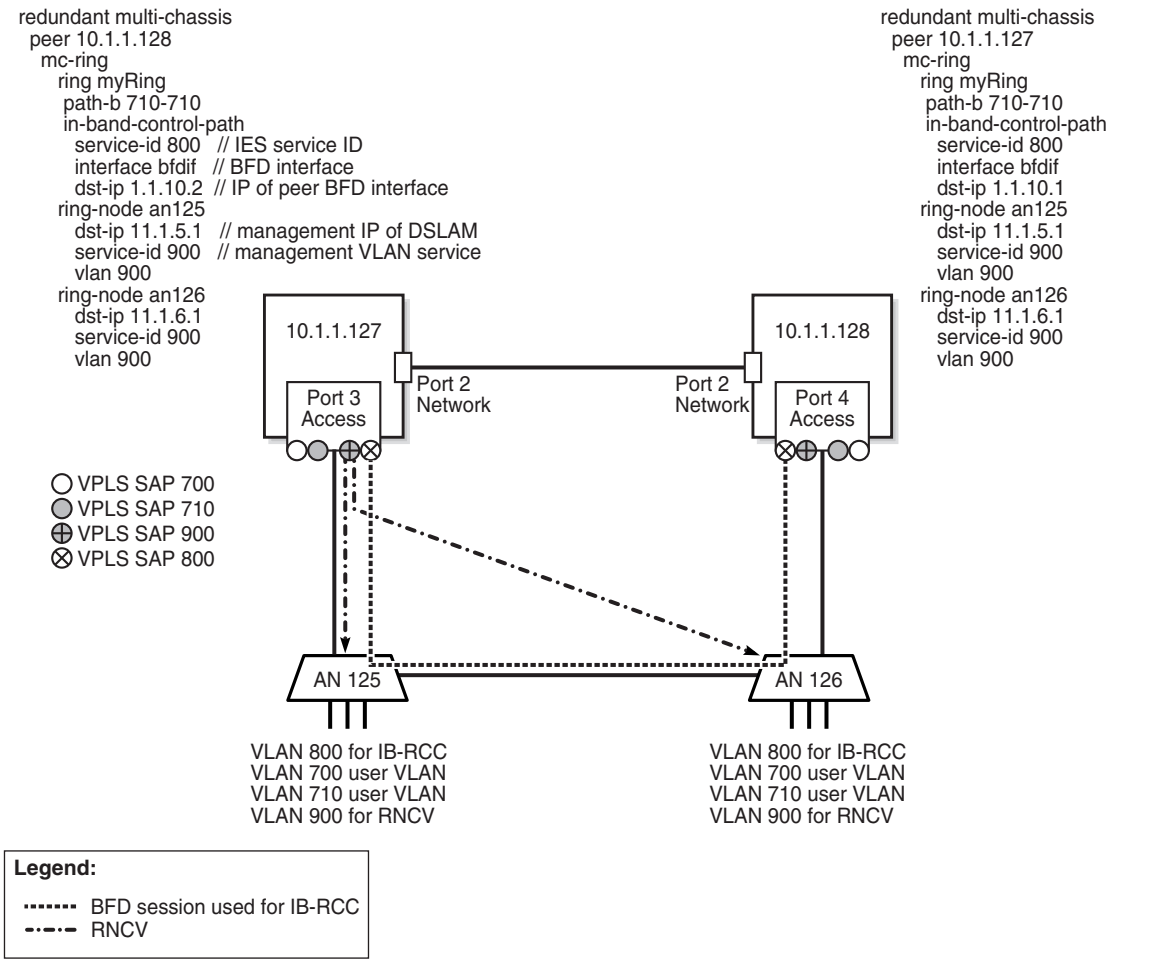
5 In the MC peer group, create an MC synchronization group that specifies each BSA access port. The MC synchronization group can synchronize the port or a VLAN range. See chapter 40 for information about MC synchronization groups.

6 Configure each ring node with the VLAN tag used for BFD to enable BFD communication through the ring. After this, each BSA SAP should be operational.

MC ring group configuration

7 Create an MC ring group that contains the BSAs (shown as 10.1.1.127 and 10.1.1.128 in Figure 41-7). For each ring node within the ring group, you must specify the management IP address of a ring node as the destination IP address and assign one VLAN for connectivity checking, shown in Figure 41-7 as VLAN 900. See Procedure 41-1 for more information.

Figure 41-7 MC ring configuration



8 Create the user VPLS and assign a SAP to each of the two BSA access ports. You can configure a protecting SAP on each BSA to provide SAP-level redundancy, if required. See chapter 68 for more information.

9 If the VPLS is to send traffic to an IES or a VPRN service, perform the following steps.

i Create a spoke SDP from each VPLS site in the MC ring group to the IES or VPRN service.

ii Configure traffic forwarding to the IES or VPRN service. See Procedure 41-2 for more information.

10 If the VPLS is to send traffic to redundant VLL Epipes, perform the following steps.

i Create a redundant VLL Epipe from each VPLS site in the MC ring group to the BSA that is the common endpoint of the VLL Epipes.

ii Configure traffic forwarding to each VLL Epipe service. See Procedure 41-3 for more information.

11 If the VPLS is to send traffic to an IES or a VPRN service, create a spoke SDP from the VPLS to the IES or VPRN service. See Procedure 41-2 for information about configuring the spoke SDP to send traffic from the MVPLS to an IES or a VPRN service.

12 Turn up the MC ring.

At this point, the following statements apply to the Figure 41-7 configuration.

- VPLS SAP 700 is operationally up on BSA 10.1.1.127 and operationally down on BSA 10.1.1.128.
- VPLS SAP 710 is operationally down on BSA 10.1.1.127 and operationally up on BSA 10.1.1.128.
- The operational state of the ring is Connected.

To test the configuration, you can shut down an access-node port in the ring to break the ring. As a result, the BSA SAPs should remain operationally up, but the operational state of the ring changes to Broken.

41.3 MC ring groups management procedures

Use the following procedures to perform MC ring group management tasks.

Procedure 41-1 To create an MC ring group



Note — You cannot create an MC ring SAP on a VPLS site that is the endpoint of redundant spoke SDPs.

1 Perform the NE preconfiguration steps in the workflow of this chapter.

2 Before you can deploy an MC ring to the participating BSAs, you must create an MC synchronization group. Perform Procedure 40-1 to create an MC synchronization group for the BSAs.

3 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

4 Choose MC Peer Group (Multi-Chassis) from the object drop-down list and click on the Search button. A list of previously created MC peer groups is displayed. See chapter 36 for information about creating MC peer groups.

5 Select an MC peer group in the list and click on the Properties button. The MC Peer Group (Edit) form opens.

6 Click on the Associated Groups tab.

7 Right-click on the MC Ring Group object and choose Create MC Ring Group from the drop-down menu. The MC Ring Group (Create) form opens.

8 Configure the parameters:

- Name
- Synchronization Tag

9 Click on the Apply button. The form displays additional tabs.

10 Click on the Properties button in the Multi-Chassis Ring on First Site panel. The MC Ring (Edit) form opens with the General tab displayed.

11 Configure the parameters:

- Interface Name
- Service ID
- Destination IP Address
- Administrative State
- Debounce Max Time (seconds)

12 Perform the following steps to create a ring node.

i Click on the Components tab.

ii Right-click on the MC Ring object and choose Create MC Ring Node. The MC Ring Node (Create) form opens.

iii Configure the parameters:

- Ring Node Name
- SAP Service ID
- SAP Outer Encapsulation Value
- SAP Inner Encapsulation Value
- Source IP Address
- Destination IP Address
- Source MAC Address
- Interval (minutes)

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The MC Ring Node (Create) form closes.

vi Repeat steps 12 ii to v to create an additional ring node, if required.

13 To configure a VLAN range for traffic that is to use the non-default path through the MC ring, perform the following steps.

i Click on the Path B VLAN Range tab.

ii Click on the Create button. The Path B VLAN Range (Create) form opens.

iii Configure the parameters:

- Start VLAN Value
- End VLAN Value

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The VLAN range entry is displayed on the MC Ring (Edit) form.

14 To configure a VLAN range for traffic that is not to be protected by the MC ring, perform the following steps.

i Click on the Exclude VLAN Range tab. The Exclude VLAN Range (Create) form opens.

ii Click on the Create button. The Path B VLAN Range (Create) form opens.

iii Configure the parameters:

- Start VLAN Value
- End VLAN Value

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The VLAN range entry is displayed on the MC Ring (Edit) form.

15 Click on the OK button. A dialog box appears.

16 Click on the Yes button. The MC Ring (Edit) form closes.

17 Click on the Properties button in the Multi-Chassis Ring on Second Site panel. The MC Ring (Edit) form opens with the General tab displayed.

18 Repeat steps 11 to 16.

19 Close the MC Ring Group (Create) form.

Procedure 41-2 To configure L3 forwarding from a VPLS or MVPLS to an IES or VPRN service

Perform this procedure to configure MC ring group traffic forwarding through a BSA spoke SDP to a BSR L3 access interface in an IES or VPRN service, as shown in Figure 41-1. See chapter 68 for information about creating and configuring VPLS and MVPLS services.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services is displayed.

3 Select the appropriate VPLS or MVPLS in the list and click on the Properties button. The service properties form opens.

4 On the navigation tree, click on a site. The site properties form opens.

5 Click on the Default Gateway tab.

6 Configure the parameters, which specify the IP and MAC address of the default gateway to which the VPLS is to forward L3 traffic.

7 Click on the OK button. The site properties form closes.

8 Click on the OK button. The service properties form closes.

Procedure 41-3 To configure an MC ring group for redundant VLL Epipe access

Perform this procedure to configure traffic forwarding from a BSA SAP in an MC ring group through a VLL Epipe to a BSA SAP outside the ring group, as shown in Figure 41-5. See chapter 67 for information about creating and configuring VLL Epipe services.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services is displayed.

3 Select the appropriate VLL Epipe service in the list and click on the Properties button. The Epipe Service (Edit) form opens.

4 On the navigation tree, right-click on an L2 access interface. The L2 Access Interface (Edit) form opens with the General tab displayed.

5 Perform one of the following to specify a ring node in the ring group that terminates on the port associated with the L2 access interface.

   a Perform the following steps to select the ring node from a list.

      i Click on the Select button in the MC Redundancy panel. The Select form opens.

      ii Select a ring node in the list and click on the OK button. The Select form closes, and the ring node name is displayed on the L2 Access Interface (Edit) form.

   b Type the name of the ring node in the MC Ring Node field.

6 Click on the OK button. The L2 Access Interface (Edit) form closes, and a dialog box appears.

7 Click on the OK button. The Epipe Service (Edit) form reappears.

8 Click on the OK button.A dialog box appears.

9 Click on the Yes button. The Epipe Service (Edit) form closes.

Procedure 41-4 To turn up the MC rings in an MC ring group



Note 1 — You cannot administratively enable an MC ring group in one operation; you must turn up the MC rings in the MC ring group individually.

Note 2 — If a Problems Encountered form is displayed when you try to turn up an MC ring, you can perform one or both of the following to view information about the problem.

- Select the listed problem and click on the Properties button.
- View the Operational State and Failure Reason fields on the State tab of the MC ring properties form.

The 5620 SAM performs a series of checks to determine whether an MC ring can be turned up. The checks include verifying the following:

- The synchronization tag is configured on the BSA.
- The VLAN-level synchronization tag is valid.
- The IES or VPRN interface for the IB-RCC is configured.
- BFD is enabled on the IB-RCC interface.
- The IES or VPRN interface is operationally up.
- The IB-RCC interface is not in use by another MC ring.
- The IB-RCC interface is on the port used for MC synchronization.
- The IB-RCC destination IP address is configured.
- The IB-RCC destination IP address is not the same as the IB-RCC source IP address.
- The IB-RCC destination IP address is not in the same subnet as the IB-RCC source IP address.
- The MVPLS or VPLS site is not configured as an endpoint for redundant spoke SDPs.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Ring Group (Multi-Chassis) from the object drop-down list and click on the Search button. A list of MC ring groups is displayed.

3 Select an MC ring group in the list and click on the Properties button. The MC Ring Group (Edit) form opens with the General tab displayed.

4 Perform one of the following.

a Turn up the MC ring using the MC ring properties form.



Note — Using this method enables you to view real-time MC ring status information while the 5620 SAM turns up the MC ring.

i Click on the Properties button beside the Site ID parameter in the Multi-Chassis Ring on First Site panel. The MC Ring (Edit) form opens.

ii Click on the State tab.

iii Set the Administrative State parameter to Up.

iv Click on the Apply button. A dialog box appears.

v Click on the Yes button. The 5620 SAM tries to turn up the MC ring.

vi View the dynamically updated information in the Operational State field.

vii Close the MC Ring (Edit) form.

viii Click on the Properties button beside the Site ID parameter in the Multi-Chassis Ring on Second Site panel. The MC Ring (Edit) form opens.

ix Repeat steps 4 a ii to vii.

b Turn up the MC ring using the navigation tree. Perform the following steps.

i Click on the Components tab.

ii Right-click on the first site object and choose Turn Up from the contextual menu. A dialog box appears.

iii Click on the Yes button. The 5620 SAM tries to turn up the MC ring.

iv Right-click on the second site object and click on the Turn Up button. A dialog box appears.

v Click on the Yes button. The 5620 SAM tries to turn up the MC ring.

5 Close the MC Ring Group (Edit) form.

Procedure 41-5 To view the operational status of MC ring group components

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Ring Group (Multi-Chassis) from the object drop-down list and click on the Search button. A list of MC ring groups is displayed.

3 Select an MC ring group in the list and click on the Properties button. The MC Ring Group (Edit) form opens with the General tab displayed.

4 Click on the Properties button beside a site that hosts an MC ring. The MC Ring (Edit) form opens.

5 Click on the State tab.

6 View the dynamically updated information in the Operational State field. The Operational State is one of the following:

- Unknown—the 5620 SAM cannot determine the operational state
- Shut Down—the MC ring is administratively down
- Config Error—the MC ring has a configuration error
- No Peer—the peer MC ring is not configured
- Connected—the MC ring is operational
- Broken—the RNCV check fails
- Local Broken—the MC ring site cannot connect to a ring node
- Conflict—the MC ring configuration conflicts with another configuration
- Testing Ring—an RNCV check is in progress
- Peer Down—the peer MC ring site is inoperable
- Waiting For Peer—the peer MC ring site is initializing

7 Click on the Components tab.

8 Right-click on a ring node object and choose Properties from the contextual menu. The MC Ring Node (Edit) form opens with the General tab displayed.

9 Click on the State tab.

10 View the dynamically updated information in the Local Operational State and Remote Operational State fields. The Operational State is one of the following:

- Unknown—the 5620 SAM cannot determine the operational state
- Not Provisioned—the ring node configuration is incomplete
- Config Error—the ring node is misconfigured
- Not Tested—no RNCV check result is available
- Testing—an RNCV check is in progress
- Connected—the ring node is operational
- Disconnected—the ring node cannot be reached

11 Close the MC Ring Node (Edit) form.

12 Close the MC Ring (Edit) form.

13 Close the MC Ring Group (Edit) form.

Procedure 41-6 To configure an MC ring peer on one NE

Perform this procedure to configure an MC ring peer when only one NE in the MC ring is managed by the 5620 SAM.



Note — This procedure assumes that you have already configured an MC peer group with an associated MC ring. If only one NE is managed by the 5620 SAM, you must create these objects from the CLI.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the NE where you want to configure an MC ring peer and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Redundancy tab.

4 Click on the MC Peer tab.

5 Configure the filter criteria, if required, and click on the Search button.

6 Choose an MC Peer in the list and click on the Properties button. The MC Peer (Edit) form opens with the General tab displayed.

7 Click on the MC Rings tab.

8 Configure the filter criteria, if required, and click on the Search button.

9 Choose an MC ring peer in the list and click on the Properties button. The MC Ring (Edit) form opens with the General tab displayed.

10 Configure the parameters:

- Interface Name
- Destination IP Address
- Administrative State
- Debounce Max Time (seconds)

11 To create a ring node, perform the following steps:

i Click on the Components tab.

ii Right-click on the MC Ring object and choose Create MC Ring Node. The MC Ring Node (Create) form opens.

iii Configure the parameters:

- Ring Node Name
- SAP Service ID
- SAP Outer Encapsulation Value
- SAP Inner Encapsulation Value
- Source IP Address
- Destination IP Address
- Source MAC Address
- Interval (minutes)

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The MC Ring Node (Create) form closes.

vi Repeat steps 11 ii to v to create an additional ring node, if required.

12 To configure a VLAN range for traffic that is to use the non-default path through the MC ring, perform the following steps:

i Click on the Path B VLAN Range tab.

ii Click on the Create button. The Path B VLAN Range (Create) form opens.

iii Configure the parameters:

- Start VLAN Value
- End VLAN Value

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The VLAN range entry is displayed on the MC Ring (Edit) form.

13 To configure a VLAN range for traffic that is not to be protected by the MC ring, perform the following steps.

i Click on the Exclude VLAN Range tab.

ii Click on the Create button. The Exclude VLAN Range (Create) form opens.

iii Configure the parameters:

- Start VLAN Value
- End VLAN Value

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The VLAN range entry is displayed on the MC Ring (Edit) form.

14 Close the MC Ring (Edit) form.

15 Close the MC Peer (Edit) form.

16 Close the Network Element (Edit) form.

Procedure 41-7 To delete an MC ring group



Caution — Deleting an MC ring group removes all of the child objects that are associated with the MC ring group, such as the following:

- MC rings
- ring nodes

Ensure that you specify the correct MC ring group for deletion in this procedure.



Note 1 — You must set the administrative state of an MC ring to Down before you can delete the MC ring.

Note 2 — Before you can set the administrative state of an MC ring to Down, you must administratively disable each VPLS or MVPLS SAP in the ring, regardless of the path they use.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Ring Group (Multi-Chassis) from the object drop-down list and click on the Search button. A list of MC ring groups is displayed.

3 Select an MC ring group in the list and click on the Properties button. The MC Ring Group (Edit) form opens with the General tab displayed.

4 Click on the Properties button beside the Site ID parameter in the Multi-Chassis Ring on First Site panel. The MC Ring (Edit) form opens.

5 Click on the State tab.

6 Set the Administrative State parameter to Down.

7 Click on the Apply button. A dialog box appears.

8 Click on the Yes button. The 5620 SAM shuts down the MC ring.

9 Close the MC Ring (Edit) form.

10 Click on the Properties button beside the Site ID parameter in the Multi-Chassis Ring on Second Site panel. The MC Ring (Edit) form opens.

11 Repeat steps 5 to 9.

12 Select the MC ring group in the list and click on the Delete button. A dialog box appears.

13 Click on the View Dependencies button. A Warning form opens.

14 View the dependency information.

15 Select the I understand the implications of this action check box.

16 Click on the Yes button. The 5620 SAM deletes the MC ring group and the corresponding configuration on each member site.

17 Close the Manage Node Redundancy form.

Policy management

42 — Policies overview

43 — QoS policies

44 — Filter policies

45 — Multicast policies

46 — Time of day policies

47 — VRRP policies

48 — Auto tunnels policies

49 — AAA policies

50 — 802.1x policies

51 — PBB MRP policies

52 — AOS Ethernet Service policies

53 — Connection profile policies

54 — Residential subscriber policies

55 — Remote network monitoring policies

56 — Constraint policies

57 — NAT policies

58 — Format and range policies

59 — PCP policies

60 — Firewall policies

42 — Policies overview

42.1 Policies overview *42-2*

42.2 Workflow to create and assign policies *42-16*

42.3 Policies procedures *42-17*

42.1 Policies overview

The 5620 SAM supports the template-based creation of rules. These rules are called policies. A 5620 SAM operator can distribute or delete policies on sites and NEs that are within their span of control.

Policies are global or local in scope. Global policies are created using the 5620 SAM. Local policies are instances of global policies that are assigned to individual NEs. Depending on the distribution mode of a local policy, when you modify a global policy using the 5620 SAM, the local instance is also updated to ensure that the policy instances are synchronized. If a local policy differs from the corresponding global policy because of changes to the global policy, a warning alarm is raised against the local policy. After a global policy is updated and distributed to the participating NEs, the 5620 SAM clears the mismatch alarms associated with the local policy.

Policy types

Service management policies specify how service traffic is handled by network resources such as interfaces, ports, daughter cards, and circuits. The policies can be used by multiple resources on multiple services. Service management policies include access ingress, access egress, MSAP policies, and network policies.

Routing management policies specify routing configuration according to specifically defined parameters. The 5620 SAM supports the following routing management policy types:

- routing
- MPLS administrative group
- VRRP priority control

Service and routing management policies are globally and seamlessly distributed to devices when they are used by resources on the device. They can also be manually distributed to devices. Subsequent changes to policies are distributed and affect all participating resources. Policy configurations can also be changed locally when you configure a network resource, for example, during service configuration or modification. These changes do not affect the global policy.

Network management policies specify how the 5620 SAM communicates with network resources, handles alarms, manages statistics, and stores information. Examples of network management policies are alarm, mediation, and accounting policies.

OmniSwitch QoS and Ethernet service policies specify how OmniSwitch devices are configured and used to provide VLAN and SVLAN services.

Time of day policies consist of time range policies and time of day suite policies. Time range policies specify multiple schedules (start and end dates and times) that you can assign to time of day suites or to ACL filter entries. A time of day suite policy is a collection of policies, such as ACL filters, access ingress and egress, and QoS schedulers, to which a time range policy has been assigned. In addition, you can assign time of day suite policies to aggregation schedulers and L2 and L3 access interfaces.

You can apply policies to resources during service creation or modification. You can also apply policies to resources before or after you configure the service by choosing and modifying the resource from the Manage Equipment or Manage Services form.

Table 42-1 describes the policies you can configure using the 5620 SAM. Unless otherwise stated in the table, the policies are described in more detail in this volume.

Table 42-1 5620 SAM policy types

Policy	Applied to	Description	Menu option
7210 Access Egress	Access port	Defines up to eight forwarding class queues and queue parameters for traffic classification. Defines forwarding class to remarking values. Maps forwarding classes to the queues.	Policies→QoS→SROS QoS→Access Egress→7210 Access Egress. See Procedure 43-5.
7210 and 1830 Access Ingress	Access SAP	Defines up to 18 forwarding class meters and meter parameters for traffic classification. Defines up to 8 HQoS ingress queues. Maps forwarding classes to the meters or queues. Defines match criteria to map flows to the meters based on any one of the criteria (IPv4, IPv6, or MAC).	Policies→QoS→SROS QoS→Access Ingress→7210 and 1830 Access Ingress. See Procedure 43-2.
7210 MPLS LSP-Exp Map	Network Interfaces	Allows separate mappings of profiles and forwarding classes on network interfaces.	Policies→QoS→SROS QoS→7210 MPLS LSP-Exp Map. See Procedure 43-28.
7210 Multipoint Bandwidth Management	7210 SAS-X	Defines the aggregate rate and up to eight forwarding class queues and queue parameters for multicast traffic.	Policies→Multicast→7210 Multicast Bandwidth Management Policies. See Procedure 45-10.
7210 and 1830 Network	Uplink port	Defines ingress dot1p to forwarding class mapping and profile state. Defines the egress queuing parameters associated with each forwarding class.	Policies→QoS→SROS QoS→Network→7210 and 1830 Network. See Procedure 43-7.
7210 and 1830 Network (1)	Network port (1)	Defines ingress dot1p or DSCP value mapping to forwarding classes. Defines unicast meters. Only unicast meters with range 1-8 are allowed. Defines the egress forwarding class to dot1p or DSCP value markings. Remarking of QoS bits.	Policies→QoS→SROS QoS→Network→7210 and 1830 Network. See Procedure 43-7.
	Network interface (1)	Defines ingress LSP-Exp value mapping to forwarding classes. Defines forwarding class to meter mapping. Defines unicast or multicast meter. Multicast meters are only supported for interface type policy. Defines the egress forwarding class to LSP-Exp value markings. Remarking of QoS bits.	
7210 and 1830 Network Queue	Uplink port	Defines forwarding class mappings to network queues and queue characteristics for the queues.	Policies→QoS→SROS QoS→Network Queue→7210 and 1830 Network Queue. See Procedure 43-13.
7210 and 1830 Port Access Egress	Access port SAP egress	Defines the SLA for service packets as they egress on the SAP.	Policies→QoS→SROS QoS→Access Egress→7210 and 1830 Port Access Egress. See Procedure 43-4.

(1 of 9)

Policy	Applied to	Description	Menu option
7210 and 1830 Port Scheduler	Access and uplink ports	Defines the parameters for the port scheduler, which allocates bandwidth to each service or subscriber that is associated with an egress port.	Policies→QoS→SROS QoS→Scheduler→7210 and 1830 Port Scheduler. See Procedure 43-19.
7210 Queue Management	Network queues	Defines the WRED slope parameters for network queues.	Policies→QoS→SROS QoS→Slope→7210 Queue Management. See Procedure 43-11.
7210 Remarking	7210 SAS QoS Policies	Defines the remarking behavior for the NE at the egress of the access SAPS, ports, and IP interfaces.	Policies→QoS→SROS QoS→7210 Remarking. See Procedure 43-27.
7210 and 1830 Slope	Access and uplink ports	Enables or disables the high-slope and low-slope parameters in the egress pool.	Policies→QoS→SROS QoS→Slope→7210 Slope. See Procedure 43-9.
7705 SAR Fabric	Daughter cards on the 7705 SAR	7705 SAR Fabric Profile policies specify the fabric shaping rate (kb/s) to the daughter card in the slot specified by the rate.	Policies→QoS→SROS QoS→7705 SAR Fabric. See Procedure 43-26.
802.1X	Ethernet ports	Defines the RADIUS server authentication policy for Ethernet ports.	Policies→Ethernet→802_1x. See Procedure 50-1.
9500 ATM QoS	Access interface	Defines the ATM classification, policing, and marking behavior for the NE.	Policies→QoS→9500 MPR QoS→9500 ATM QoS. See the *5620 SAM MPR User Guide* for more information.
9500 Radio Interface Queue Map	Access interface	Defines the values for queue size and queue delay for all queues for the radio Interface connected to the NE.	Policies→QoS→9500 MPR QoS→ 9500 Radio Interface Queue Map. See the *5620 SAM MPR User Guide* for more information.
9500 NE QoS	Network interface	Defines the QoS parameters for the NE including the mapping between forwarding classes and queues, and the parameters associated with the different queues.	Policies→QoS→9500 MPR QoS→ 9500 NE QoS. See the *5620 SAM MPR User Guide* for more information.
Accounting	Network interface Access interface Circuit	Manages accounting policies.	Tools→Statistics→Accounting. See the *5620 SAM Statistics Management Guide* for more information.
Access Egress	Access interface	Defines egress classification, policing, shaping, and marking on the egress side of the interface.	Policies→QoS→SROS QoS→Access Egress→Access Egress. See Procedure 43-3.
Access Ingress	Access interface	Defines ingress classification, policing, shaping, and marking on the ingress side of the interface.	Policies→QoS→SROS QoS→Access Ingress→Access Ingress. See Procedure 43-1.
ACL IP Filter	Network interface Access interface Circuit	Controls network traffic into or out of an interface or circuit based on IPv4 matching criteria.	Policies→Filter→ACL IP Filter. See Procedure 44-2.
ACL IPv6 Filter	Network interface Access interface Circuit	Controls network traffic into or out of an interface or circuit based on IPv6 matching criteria.	Policies→Filter→ACL IPv6 Filter. See Procedure 44-3.
ACL MAC Filter	Access interface Circuit	Controls network traffic into or out of an interface or circuit based on MAC matching criteria.	Policies→Filter→ACL MAC Filter. See Procedure 44-1.
ACL VLAN Filter	Access interface	Allows or denies VLAN ranges that are forwarded on the network ports of a ring card.	Policies→Filter→ACL VLAN Filter. See Procedure 44-4.

(2 of 9)

Policy	Applied to	Description	Menu option
Admin Group (MPLS)	MPLS interfaces LSPs LSP paths	Configures MPLS administrative groups and defines the groups to which an MPLS interface, LSP, or LSP path belongs.	Policies→MPLS→MPLS Administrative Group. See Procedure 22-21.
Advanced Configuration	Queues Policers	Allows for additional configurations to queues and policers in the access ingress/egress policies and the ingress/egress queue group templates.	Policies→QoS→SROS QoS→Scheduler→Advanced Configuration Policy. See Procedure 43-25.
Alarm	Alarm logs Alarms	Defines how the 5620 SAM handles individual incoming alarms, and how alarm logs are created and stored.	Administration→Alarm Settings. See Procedures 31-1, 31-3, 31-5, and 31-11.
ANCP Policy	L2 and L3 access interfaces	Defines the behavior of the residential subscriber host with which the policy is associated.	Policies→Residential Subscriber. See Procedure 54-2.
Application Assurance	7450 ESS, 7750 MG, and 7750 SR	Used to enable services that enhance the hierarchical per-subscriber, per-service, and per-application QoS functions.	Policies→ISA Policies→Application Assurance. See chapter 76.
ATM QoS	Access interface	Defines ATM ingress and egress classification, policing, shaping, and marking	Policies→QoS→SROS QoS→ATM QoS. See Procedure 43-33.
BGP Peering	Residential subscriber host	Applies BGP peering configuration to residential subscriber host.	Policies→Residential Subscriber. See Procedure 54-10.
Block Reservation	5620 SAM LI users	Used to reserve a filter entry block in the base ACL MAC filter for LI MAC Filter entries.	Policies→Filter→LI Policies→Block Reservation. See Procedure 44-9.
Category Map Policy	Credit control policy and SLA profile	Defines categories that monitor usage information based on volume or time.	Policies→Residential Subscriber. See Procedure 54-7.
Connection Profile	ATM channel	Defines a list of VPI/VCI pairs.	Policies→ATM→Connection Profile. See Procedure 53-1.
CPM Filter	Device	Allows you to create or modify a CPM filter policy for a managed device to specify which types of traffic to accept or deny, and to allocate and rate-limit the shaping queues for the traffic directed to the CPMs.	Security→NE CPM Filter. See the *5620 SAM System Administrator Guide*.
Credit Control Policy	SLA profile	Defines out-of-credit and error control actions for a category map.	Policies→Residential Subscriber. See Procedure 54-8.
DHCP filter	Access interface Circuit	Controls network traffic into or out of an interface or circuit based on DHCP matching criteria.	Policies→Filter→DHCP Filter. See Procedure 44-7.
Diameter	Residential Subscriber	Specifies common diameter protocol parameters to be inherited by associated diameter peers.	Policies→Residential Subscriber. See Procedure 54-11.
Dynamic Service Policy	—	Associates a RADIUS script policy with a CLI user, SAP limit, and up to two accounting policies. Referenced by RADIUS CoA messages during dynamic service creation.	Policies→Dynamic Service Policy. See Procedure 75-1.
Egress Multicast Group	L2 access interfaces	Groups destination SAPs in a chain which receives a single multicast packet from the egress forwarding plane with only a single pass.	Policies→Multicast→Egress Multicast Group. See Procedure 45-1.
Egress Queue Group Template	Access interface	Used for Access Egress Queue Group and Network Egress Queue Group creations on Ethernet ports.	Policies→QoS→SROS QoS→Queue Group→Egress Template. See Procedure 43-24.

(3 of 9)

Policy	Applied to	Description	Menu option
Ethernet CFM	Ethernet services	Defines the Maintenance Domain for Ethernet services (VPLS, EPIPE, VPRN and IES) including SAP and SDP bindings.	Tools→Ethernet CFM→Maintenance Domain Policies. See Procedure 78-1.
Ethernet Service	SAPs and UNI ports	A SAP is associated with a stacked VLAN service. A SAP profile defines values for ingress bandwidth sharing, rate limiting, customer VLAN tag processing (translate or preserve), and priority mapping (inner to outer tag or fixed value). A UNI profile is associated with a UNI port and configures how a variety of protocol control packets are processed on the UNI port. Processing actions include Tunnel, Drop, Peer, and MAC Tunnel.	Policies→Ethernet→AOS Ethernet Service. See Procedures 52-1 and 52-2
File	—	Manages files on the device. See the *5620 SAM Statistics Management Guide* for more information.	Tools→Statistics→File Policies See the *5620 SAM Statistics Management Guide* for more information.
Firewall	Layer 3 interfaces Network interfaces Management interfaces	The firewall supported on the 7705 SAR-H applies a firewall policy to an interface. You can configure Host Group, Rule Set, Service Group and Zone firewall policies on the interfaces. You can also configure a firewall log policy and associate it with a rule set.	Policies→Firewall. See Procedures 60-1, 60-2, 60-3, 60-4 and 60-5.
Format Policy	All services, LSPs, L2 and L3 access interfaces	Specifies the text format of names and descriptions of services, LSPs, L2 and L3 access interfaces. Format policies must be associated with users and user groups.	Administration→Format and Range Policies. See Procedure 58-1.
Host Lockout Policy	L2 and L3 access interfaces	Defines lockout parameters for misconfigured or malicious subscribers that are continuously trying to connect.	Policies→Residential Subscriber. See Procedure 54-14.
Host Tracking Policy	Subscriber profiles	Allows subscriber video traffic to be included in the egress rate control for the subscriber.	Policies→Residential Subscriber. See Procedure 54-6.
HSMDA Pool Policy	HSMDAs	Controls how buffers are distributed between HSMDA pools.	Policies→QoS→SROS QoS→Buffer Pool→HSMDA Pool. See Procedure 43-29.
HSMDA WRR Policy	L2 and L3 access interfaces	Specifies the weighted round robin parameters for network queues.	Policies→QoS→SROS QoS→Scheduler→HSMDA WRR Policy. See Procedure 43-17.
IGMP	Subscriber profile	Associates subscriber profiles with static multicast group and static source IP addresses.	Policies→Residential Subscriber. See Procedure 54-9.
IKE Policy	IPsec tunnels IPsec gateways	Negotiates IPsec security associations between IPsec peers.	Policies→ISA Policies→IKE. See Procedure 29-1.
Ingress Multicast Bandwidth Policy	MDAs	Manages the ingress multicast path bandwidth of multicast forwarding paths into the switching fabric.	Policies→Multicast→Ingress Multicast Path Management. See Procedure 45-5.
Ingress Multicast Information Policy	Routing instance	Defines how each multicast channel is handled by NEs.	Policies→Multicast→Ingress Multicast Path Management. See Procedure 45-3.

(4 of 9)

Policy	Applied to	Description	Menu option
Ingress Multicast Reporting Destination Policy	Residential subscriber IGMP policies	Specifies the destination server for the collection of multicast reports.	Policies→Multicast→Ingress Multicast Path Management. See Procedure 45-4.
Ingress Queue Group Template	Access interface	Used for Access Ingress Queue Group creation on Ethernet access ports.	Policies→QoS→SROS QoS→Queue Group→Ingress Template. See Procedure 43-23.
ISA-IPSec Transform and IPsec security	IPsec tunnels IPsec security associations IPsec tunnel templates	Specifies the protocol for the IPsec authentication header and the encryption protocol for the encapsulating security payload, or ESP, and defines the attributes that are used to secure the data.	Policies→ISA Policies→IPSec Transform. See Procedures 29-2, 29-4, and 29-5.
ISA-IPSec Static Security Association	OSPFv3 interfaces Virtual links	Defines the SPI values, algorithms, protocol, and keys to be used.	Policies→ISA Policies→IPSec Static Security Association. See Procedure 29-3.
ISA-IPSec Tunnel Template	IPsec gateways	Configures shared IPsec transform and IKE policies.	Policies→ISA Policies→IPSec Tunnel Template. See Procedure 29-4.
L2TP RADIUS Accounting Policy	L2TP tunnel L2TP session	Collects usage data based on either an L2TP tunnel or an L2TP session and sends this information to a RADIUS server.	Policies→AAA Policies→L2TP RADIUS Accounting. See Procedure 49-3.
LI MAC filter	5620 SAM LI users	Used to filter out traffic to non-LI users for LI mirror services.	Policies→Filter→LI Policies→LI MAC filter. See Procedure 44-8.
LSP Template MVPN	P2MP LSPs	Configures a template for P2MP LSP parameters.	Policies→MPLS→LSP Template MVPN. See Procedure 25-23.
LTE Profiles and Policies	—	See the *5620 SAM LTE EPC User Guide*.	Policies→Mobile→LTE Profiles and Policies. See the *5620 SAM LTE EPC User Guide*.
Manage auto tunnel rules	—	Create and configure auto-tunnel rules.	Policies→Auto Tunnels→Auto Tunnel Rules. See Procedures 48-2, 48-3, 48-4, 48-5, 48-6, 48-7 and 48-8.
Mediation	5620 SAM	Defines how the 5620 SAM polls the network.	Administration→Mediation. See Procedure 10-4.
MCFR Ingress QoS Profile	MLFR bundles	Create and configure user-defined ingress QoS profiles for MLFR bundles.	Policies→QoS→SROS QoS→MCFR→Ingress QoS Profile. See Procedure 43-40.
MCFR Egress QoS Profile	MLFR bundles	Create and configure user-defined egress QoS profiles for MLFR bundles.	Policies→QoS→SROS QoS→MCFR→Egress QoS Profile. See Procedure 43-41.
MC MLPPP Ingress QoS Profile	APS and ASAP MLPPP bundles	Create and configure user-defined ingress QoS profiles for MC MLPPP bundles.	Policies→QoS→SROS QoS→MLPPP→Ingress QoS Profile. See Procedure 43-38.
MC MLPPP Egress QoS Profile	APS and ASAP MLPPP bundles	Create and configure user-defined egress QoS profiles for MC MLPPP bundles.	Policies→QoS→SROS QoS→MLPPP→Egress QoS Profile. See Procedure 43-39.

(5 of 9)

Policy	Applied to	Description	Menu option
WMM Profiles and Policies	9471 WMM instances and reference points	An WMM emergency number list profile specifies the emergency services that are associated with a set of emergency telephone digits. An WMM SCTP profile specifies SCTP configurations between S1-MME peers. An WMM GTP profile specifies GTP configurations between S11 peers.	Policies→Mobile→WMM Profiles and Policies. See the *5620 SAM LTE EPC User Guide*.
Mobile Gateway Profile	PGW or GGSN	Configures a signaling interface between the WLAN-GW and the mobile gateway.	Policies→Residential Subscriber. See Procedure 54-13.
MSAP	Capture SAPs L2 access interfaces MSAPs L2 and L3 access interfaces	Specifies how parameters are applied in the creation of an MSAP.	Policies→Residential Subscriber. See Procedure 54-5.
Multicast CAC	Network interfaces	Controls the bandwidth consumed by BTW distribution services.	Policies→Multicast→Multicast CAC. See Procedure 45-2.
Multicast Package	Broadcast TV VLAN services	Defines the set of broadcast channels that are multicast across a ring group in a BTV VLAN.	Policies→Multicast→Multicast Package. See Procedure 45-9.
Multicast Package	VPLS instance	Assigns a common set of multicast groups to all 7450 ESS, 7750 SR, or 7950 XRS NEs in an MVR VPLS.	Policies→Multicast→Multicast Package. See Procedure 45-9.
NAT	Routing instances	Allows you to create and manage NAT policies that define general NAT properties and associate a NAT address pool with an ISA-NAT group on the same NE.	Policies→ISA Policies→NAT. See Procedure 24-2.
NAT RADIUS Accounting	NAT ISA group	Allows you to configure access to a group of RADIUS servers.	Policies→AAA Policies→NAT RADIUS Accounting. See Procedure 49-2.
Named Pool Buffer	Network daughter card and network port	Allows the operator to override the default pool allocation behavior.	Policies→QoS→SROS QoS→Buffer Pool→Named Buffer Pool. See Procedure 43-22.
NE AOS Security Authentication	Network Element	Allows you to create a RADIUS or TACACS+ security policy for an AOL.	Administration→Security→NE AOS Security Authentication. See the *5620 SAM System Administrator Guide*.
NE Deployment, Backup, Software Upgrade	5620 SAM	Defines how the 5620 SAM communicates with the network.	Administration→NE Maintenance. See the *5620 SAM System Administrator Guide* for more information.
NE DoS Protection	Access interface	Allows you to create a policy to control the amount of subscriber-based control-plane traffic that NE interfaces receive.	Administration→Security→NE DoS Protection. See the *5620 SAM System Administrator Guide* for more information.
NE DDoS Protection	Access Interface	Allows you to create a policy to control the amount of traffic that NE interfaces receive by isolating protocols and subscribers.	Administration→Security→NE DDoS Protection. See the *5620 SAM System Administrator Guide* for more information
NE Password Policy	Network Element	Allows you to create a policy that specifies the rules to which a password must conform on one or more devices.	Administration→Security→NE Password Policy. See the *5620 SAM System Administrator Guide* for more information.

(6 of 9)

Policy	Applied to	Description	Menu option
NE PKI Certificate Authority profile	Network Element	Allows you to create and distribute a CA Profile policy which is used to certify the authenticity of users.	Administration→Security→NE PKI Authentication→PKI Certificate Authority Profiles. See the *5620 SAM System Administrator Guide* for more information.
NE RADIUS Authentication	Network Element	Allows you to create a policy that configures RADIUS parameters to control access to the managed device.	Administration→Security→NE RADIUS Authentication. See the *5620 SAM System Administrator Guide* for more information.
NE TACACS+ Authentication	Network Element	Allows you to create a policy that configures TACACS+ parameters to control access to the managed device.	Administration→Security→NE TACACS+ Authentication. See the *5620 SAM System Administrator Guide* for more information.
Network	Network interface	Defines egress QoS marking and ingress QoS interpretation for traffic on core network IP interfaces.	Policies→QoS→SROS QoS→Network→Network. See Procedure 43-6.
Network Queue	Network daughter card Network port	Defines the default burst allocations for queues based on the queue's forwarding class.	Policies→QoS→SROS QoS→Network Queue→Network Queue. See Procedure 43-12.
PBB MRP	Ethernet ports	Limits the scope of MMRP advertisements to a specific network domain using ISID-based filters for both the MMRP control plane and the B-VPLS data plane.	Policies→Ethernet→PBB MRP. See Procedure 51-1.
PCP	NAT PCP server	Configures static port forwards, collects information about port forwards, and obtains the outside IP address from software that is installed on the home network or on the CPE.	Policies→ISA Policies→NAT. See Procedure 59-1.
Policer Control	Ingress or egress SAPs Subscriber Contexts	Provides control hierarchy for policer objects configured on SAPs or subscriber contexts.	Policies→QoS→SROS QoS→Scheduler→Policer Control. See Procedure 43-20.
Policy Sync Group	AA Group Policy	Designate an AA group policy as the master policy and add one or more AA group policies to Policy Sync Group members. Overwrite or add the contents of the master policy to one or more of its members.	Policies→Policy Sync Group. See Procedure 76-6.
Port Policy	ISA virtual ports	Assigns a port scheduler policy to an ISA virtual port.	Policies→QoS→SROS QoS→Scheduler→Port Policy. See Procedure 43-21.
Port Scheduler	Egress ports and channels	Defines hierarchical bandwidth allocation and scheduling at the egress port level.	Policies→QoS→SROS QoS→Scheduler→Port Scheduler. See Procedure 43-18.
PPP Policy	Access interfaces	Defines PPP parameters for an access interface.	Policies→Residential Subscriber. See Procedure 54-4.
PPPoE Policy	Access interfaces	Defines PPPoE parameters for an access interface.	Policies→Residential Subscriber. See Procedure 54-3.
QoS	VLAN and stacked VLAN services	QoS policies are used for traffic prioritization, bandwidth shaping, and Layers 2, 3, and 4 filtering.	Policies→QoS→AOS QoS Policies. See Procedures 43-34, 43-35, 43-36 and 43-37 for more information.
RADIUS Accounting Policy	Subscriber profiles	Sends accounting information to the RADIUS server when a subscriber logs in or logs out of a session.	Policies→RADIUS Based Accounting. See Procedure 49-1.

(7 of 9)

Policy	Applied to	Description	Menu option
RADIUS Script	RADIUS server	References python scripts for RADIUS AAA packet manipulation in a subscriber management application.	Policies→AAA Policies→RADIUS Script. See Procedure 54-16.
RADIUS Server	RADIUS server	Configures a group of RADIUS servers.	Policies→AAA Policies→RADIUS Server. See Procedure 49-4.
RADIUS / TACACS+ User Authentication	User	Allows you to create RADIUS and TACACS+ authentication policies to control access to managed devices for 5620 SAM user accounts.	Security→5620 SAM RADIUS/TACACS+ User Authentication. See the *5620 SAM System Administrator Guide* for more information.
RAN Profiles and Policies	Reference point	See the *5620 SAM LTE EPC User Guide*.	Policies→Mobile→RAN Profiles and Policies. See the *5620 SAM LTE EPC User Guide*.
Range Policy	All services, LSPs, L2 and L3 access interfaces	Specifies the ID number range for services, LSPs, L2 and L3 access interfaces. Range policies must be associated with users and user groups.	Administration→Format and Range Policies. See Procedure 58-2.
RCA Audit Policy	VLL, VPLS, and VPRN services and physical links	Allows you to create and manage RCA audit policies that define which policy types to execute to identify problems with the configuration of different service and physical links.	Policies→RCA Audits. See Procedure 80-1.
Remote Network Monitoring	5620 SAM	Maps remote network monitoring events to information alarms in the 5620 SAM GUI.	Tools→Remote Network Monitoring (RMON). See Procedure 55-1.
Route Download	RADIUS server	Downloads customer-assigned subnets from a RADIUS server to an NE.	Policies→AAA Policies→Route Download. See Procedure 49-7.
Routing	Routing instance	Controls the size and content of routing tables, advertised routes, and best routes.	Policies→Routing→Statement. See Procedure 22-15. Policies→Routing→Prefix List. See Procedures 22-16 and 22-29 Policies→Routing→Community. See Procedures 22-17 and 22-29. Policies→Routing→Damping. See Procedures 22-18 and 22-29. Policies→Routing→AS Path. See Procedure 22-19. Policies→Routing→AS Path Group. See Procedure 22-20.
Rule-based groups	—	Groups NEs in ordered or unordered rule-based tunnel policies.	Policies→Auto Tunnels→Rule-Based Groups. See Procedure 48-1.
Scheduler	Access ingress interface Access egress interface	Defines hierarchical rate limiting and scheduling to govern queue scheduling.	Policies→QoS→SROS QoS→Scheduler→Scheduler. See Procedures 43-15 and Section 61.5. Policies→QoS→SROS QoS→Scheduler→HSMDA Scheduler. See Procedure 43-16.
Shared Queue	Network daughter card	Defines distribution of traffic over core network.	Policies→QoS→SROS QoS→Shared Queue. See Procedure 43-14.
Shared Risk Link Group	MPLS interfaces LSP paths	Configures Shared Risk Link Groups and associates the groups to one or more MPLS interfaces.	Policies→MPLS→ Shared Risk Link Group. See Procedures 22-22.

(8 of 9)

Policy	Applied to	Description	Menu option
Shared Risk Link Group Static Configuration	MPLS interfaces LSP paths	Configures Shared Risk Link Groups and allows you to manually enter into the SRLG database the SRLD membership for links in the entire network.	Policies→MPLS→ Shared Risk Link Group Static Configuration. See Procedures 22-23.
Size Constraint policy	—	Allows you to create size constraint policies that regulate the number of historical records retained in the 5620 SAM database.	Administration→Constraint Policies→Size Constraint Policies. See Procedure 56-1.
Ageout Constraint policy	—	Allows you to configure a qualified ageout interval for a specified object type, after which objects are deleted from the 5620 SAM database.	Administration→Constraint Policies→Ageout Constraint Policies. See Procedure 56-2.
SLA Profile	SAPs	Defines the resources that an NE assigns to a particular subset of subscriber hosts.	Policies→Residential Subscriber. See Procedure 54-17.
Slope	Access port Network daughter card Network port	Defines high priority and low priority RED slope characteristics for buffer pools.	Policies→QoS→SROS QoS→Slope→WRED Slope. See Procedure 43-8. Policies→QoS→SROS QoS→Slope→HSMDA WRED Slope. See Procedure 43-10.
Software Upgrade policy	Network Element	Allows you to: • create a 5620 SAM device software upgrade policy • perform an immediate upgrade or schedule an upgrade on a device • monitor the status of an upgrade • import and export a device software image	Administration→NE Maintenance→Software Upgrade. See the *5620 SAM System Administrator Guide* for more information.
SSM Translate	Routers	Allows the receiver of multicast packets to specify desired source addresses to the router.	Policies→Multicast→SSM Translate. See Procedure 45-6.
Subscriber Authentication	VPLS or IES SAP or group interface	Grants network access to a dynamic host.	Policies→AAA Policies→Subscriber Authentication. See the *5620 SAM System Administrator Guide* for more information.
Subscriber identification	SAP	Associates residential subscriber hosts with subscribers for the allocation of network resources.	Policies→Residential Subscriber. See Procedure 65-23.
Subscriber Multicast CAC Policy	Subscriber profiles	Defines bandwidth constraints for multicast CAC.	Policies→Residential Subscriber. See Procedure 54-12.
Subscriber Profile	NEs and SAPs	Defines the aggregate HQoS and accounting characteristics for the hosts of a specific subscriber.	Policies→Residential Subscriber. See Procedure 54-18.
Time of Day Suite	Aggregation scheduler policies and L2 and L3 access interfaces	A collection of policies, such as ACL filters, access ingress and egress, and QoS schedulers, to which time range policies have been assigned.	Policies→Time of Day→Time Of Day Suite. See Procedure 46-2.
Time Range	Time of day suite policy entries and ACL filter policy entries	Specifies multiple schedules that can be used by time of day suite policies or ACL filter policies.	Policies→Time of Day→Time Range. See Procedure 46-1.
VRRP	VRRP instance	Applies a VRRP priority-control policy to non-owner VRRP instances in a virtual router.	Policies→VRRP. See Procedure 47-1.

(9 of 9)

Note
(1) Applies to the 7210 SAS-M24F, 7210 SAS-M24F2XFP, and 7210 SAS-M24F2XFP [ETR].

Global policies

When there is no global policy associated with a local policy, the 5620 SAM automatically creates a global policy that is identical to the first discovered local policy. If the local policy is incomplete, the 5620 SAM creates an incomplete global policy. The following read-only parameters describe the initialization phases of a global policy:

- Discovery State
  - In Progress—The global policy is created as part of a specific NE resynchronization during the full NE resynchronization or NE discovery. The global policy does not yet match any local policy and is waiting for completion.
  - Completed—At the end of the full NE resynchronization, when the resynchronization is successful, the global policy is completely updated from the first discovered local policy.
  - Failed—At the end of the full NE resynchronization, if the resynchronization is not successful, the global policy is not updated from the first discovered local policy. A failed global policy is updated during the next successful full NE resynchronization, or the policy can be manually synchronized with a specific local policy. The global policy remains in the Failed state after a 5620 SAM server failure or activity switch.
  - Initialize—The global policy is created by SNMP trap notification. The global policy may need to be manually synchronized with the specific local policy.
  - N/A (default)—The global policy is created or modified by a 5620 SAM user.
- Origin

  The Origin information field denotes the NE that causes the creation of the global policy. It does not change if the policy is then modified at a later date. If the global policy is created from the 5620 SAM, the originator is shown as Admin.
  - Site ID—The global policy is created as part of a specific NE resynchronization or by SNMP notification.
  - User Name—The global policy is created by a 5620 SAM user.



Note 1 — If you attempt to modify a global policy with an “In Progress” Discovery State, the following occurs:

- When discovery or full resynchronization of the NE is ongoing, the modification fails.
- When discovery or full resynchronization of the NE is completed, modifications using OSS proceed, although a warning appears and allows you to cancel the modification. If the modification is not cancelled, the Discovery State is changed to N/A, and the global policy is not updated to match the local policy.
- When a global policy is modified, the Discovery State is reset to N/A.

Note 2 — At any time during discovery or a full resynchronization, you can use the SyncTo method from OSS or synchronize the global policy from any local policy.

When a discovery or full resynchronization of an NE fails and there is no 5620 SAM server failure or activity switch, all global policies that are waiting for completion are changed to Failed for the Discovery State. If you start another full resynchronization of the failed NE, the 5620 SAM tries again to complete the global policies from the NE that is part of the resynchronization and which has the Failed or In Progress Discovery State. The 5620 SAM also attempts completion of the synchronization of global policies that have a Failed or an In Progress State until a server failure or an activity switch occurs.

Table 42-2 describes the recommended operator actions to recover global policies when the Discovery State remains In Progress or Failed.

Table 42-2 Actions to recover global policies

Discovery State	5620 SAM server failure	NE state	Recovery action
In Progress/Failed	No	Resync Failed	Retry a full resynchronization or synchronization from another local policy
In Progress/Failed	No/Yes	Removed/Unmanaged	Synchronization from another local policy
In Progress/Failed	Yes	Resync Completed	Synchronization from another local policy
In Progress/Failed	Yes	Resync Failed	Retry a full resynchronization and synchronization from another local policy

Policy distribution

The 5620 SAM supports the partial distribution of global policies. Before a global policy is distributed to the NEs, the 5620 SAM determines whether the global policy, policy properties, and the policy entries are applicable for each NE to which the policy is to be applied. If an NE does not support the policy, property, or entry defined in a global policy, the policy is partially distributed to the NE. The inapplicable policy, property, or entry is not distributed to the NE. An alarm is not raised if a policy is partially distributed. When you use the 5620 SAM GUI or OSS, failure of distribution to an NE does not affect distribution to other NEs.

The 5620 SAM creates a global policy in Draft mode. This allows you to verify that the policy is correctly configured before distributing it to the NEs. When a policy is approved for distribution, you change its configuration mode to Released. Whether you're dealing with a new or existing policy, changing its mode to Released opens the Distribute window. If the policy was previously distributed to a group of NEs, then only those NEs are shown in the Distribute window. By default, all the NEs are selected in the window. You can deselect the NEs you want, or use the current selection to distribute the policy. If the policy was not previously distributed, or its local versions are non-existent (deleted either by a user or an NE), then the Distribute window displays a list of compatible NEs. You must then select which NEs to distribute the policy to. Alternatively, you can use the drop-down menu in the Distribute window to select a Policy Distribute Group for the distribution.

You can monitor policy distribution either in the Distribute window or by using the Task Manager. The 5620 SAM saves the latest released version of the global policy. If you select a Policy Distribute Group, the NEs contained within the group will be shown in the Selected Objects panel once the distribution begins. This allows you to monitor the distribution progress at the individual NE level.

The 5620 SAM supports the ability to scale policy deployment. If you release a large global policy to multiple NEs using one deployer, you may degrade system performance. An operator can configure the maximum number of objects that a deployer can send. The 5620 SAM uses this value to calculate how many NEs can be deployed per deployer. The default value is 10 000 objects per deployer. Table 42-3 provides an example of possible parameter settings to deploy a global policy that contains 1000 objects.

In the example below, there is one deployer per site. When the parameter setting is less than the number of entries in the policy, the 5620 SAM does not use more than one deployer for one site. If the parameter setting is too high, the 5620 SAM uses one deployer for all sites which may impact system performance. See Procedure 42-13 for more information about configuring the maximum number of objects per deployer.

Table 42-3 Example of policy deployment

Policy distribution maximum number of objects per deployer	Number of objects in a global policy	Maximum number of sites per deployer
0	–	All sites
1	–	1 site
500	1000	1 site
1000	1000	1 site
5000	1000	5 sites
10 000	1000	10 sites
100 000	1000	100 sites

Policy audits

To identify local and global policy mismatches, you can perform a policy audit that compares the local and global instances of a policy, and then review the differences. An audit can be performed on local policies of NEs that are in the user span of control and policies that the user license supports.

You can audit all policies in the network or on selected NEs in the following ways:

- by policy group
- by policy type
- by global policy

If an entry exists in both the global and a local version of a policy but a field within that entry is different between the versions, then the audit indicates exactly which field is different. This includes missing entries as well. See Procedures 42-10 and 42-12 for information about identifying policy discrepancies using a policy audit.

If there is a mismatch between a local policy instance and the global instance, an alarm is raised against the local policy. The 5620 SAM clears the alarms from previous audits if the mismatch condition no longer exists.



Warning — Alcatel-Lucent recommends that you change a policy on an NE using only the 5620 SAM or an OSS client. This ensures that there is no mismatch in policy IDs or policy configurations between the managed NEs and the 5620 SAM.

Creating or modifying a policy using a CLI may lead to inconsistencies in the policy configuration throughout the network.

Depending on the results of an audit, the mode of the local policy may change. If the audit discovers differences between the local and global policies, you can change the mode to allow only local configuration. When the audit discovers that the local policy and global policy match, the local mode can be changed to synchronize with global policies. For example, when you need the 5620 SAM to discover new NEs, set the mode parameter to local configuration only to ensure that unique policies are not modified when a global policy is updated. The audit results can be reviewed to determine whether a policy should remain local.

Policy overrides

With some policy types, you can use the 5620 SAM to configure a policy override that allows you to change or override the default settings associated with the policy.

For policy types that allow multiple overrides to be configured, the Override Policy Items tab on the policy creation form displays all of the subordinate override policies that are configured on the policy. Each override policy is displayed on their own sub-tabs under the Override Policy Items tab. The override policies that appear on the GUI are dynamic, based on the policy type to be configured.

The following policy types aggregate all subordinate override policies on the Override Policy Items tab.

- SLA Profile policies
- Subscriber Profiles policies
- Port policies
- Services (SAP) policies
- HSMDA Scheduler policies

42.2 Workflow to create and assign policies

1 As required, configure policy system preferences to customize or change the default value to meet your operational requirements. See the *5620 SAM System Administrator Guide* for more information. You can customize the following policy system preferences.

   a Enforce a restriction in the distribution mode for certain types of local policies that will permit local editing only.

   b Enforce a restriction in the distribution mode for certain types of local policies that will cause changes made to a local policy using CLI to set the distribution mode to Local Edit Only.

   c Enable access ingress and access egress policy names, and ACL IP, ACL IPv6, and ACL MAC policy filter names to be displayed on the policy configuration form.

2 Create the required policies. Table 42-1 describes the policies that are configured using the 5620 SAM.

3 Distribute the policies. See Procedure 42-1 for more information.



Note 1 — You do not need to explicitly distribute a policy; a policy is distributed to a device when it is assigned to a resource on the device.

Note 2 — When you distribute a policy to a 7705 SAR, all values within that policy must be supported by that 7705 SAR; otherwise, the distribution of the policy to that 7705 SAR is blocked.

4 Assign policies to resources during service configuration or modification. See Chapter 61 for more information.

5 As required, modify the policy. Perform Procedure 42-4.

6 As required, delete the policy. Perform Procedure 42-5.

   A QoS, ACL, or an AA transit IP policy cannot be deleted until it is removed from the all SAPs or network ports where it is applied. When a policy is deleted, it is removed from the 5620 SAM, including the database and all devices.

   Do not delete a routing policy from an NE that is associated with one or more services. Multiple services on the NE may use the policy.

7 As required, copy or overwrite the policy. Perform Procedure 42-6.

8 As required, synchronize the policy to specify the local policy entry as global and redistribute it across all deployed associations. Perform Procedure 42-7.

9 As required, perform a policy audit to compare all local policies with the associated global policies. Perform Procedure 42-8. To perform a policy audit for multiple global policies with same type, perform Procedure 42-9.

10 As required, perform a policy audit of the global policy to compare all local policies with the associated global policy. Perform Procedure 42-10.

11 As required, identify differences between a global policy and a local policy or two local policies. Perform Procedure 42-12.

12 As required, specify the maximum number of NEs to which a policy is distributed by one deployer. Perform Procedure 42-13.

42.3 Policies procedures

Use the following procedures to perform 5620 SAM policies tasks.

Procedure 42-1 To distribute a policy

Use this procedure to distribute a policy used by network resources and to configure the distribution mode of local policies. Policies are also distributed to a device when the policy is assigned to a resource on that device.



Note — When you distribute a global policy:

- A policy must first be released to an NE before it can be distributed to that NE.
- Local NE versions of policies that use the Sync With Global distribution mode will allow the NE to receive the distribution of a global policy.
- Local NE versions of policies that use the Local Edit Only distribution mode will not allow the NE to receive the distribution of a global policy. You must ensure that the policy distribution mode for the local policy is set to Sync With Global if you want the NE to receive the distribution of a global policy.
- The default behavior when you release a policy for distribution is that the Distribute window opens and allows you to select the NEs required for distribution. Alternatively, you can enable a parameter setting in the System Preferences that will upon release of the global policy, automatically distribute it to NEs that already have local versions of the policy. Refer to the *5620 SAM System Administrator Guide* and *5620 SAM Parameter Guide* for more information on the use of the Auto Distribute Global Policy when Released parameter.
- Local SR-family NE versions of policies that are changed using CLI can have their distribution modes automatically set to either Sync with Global or Local Edit Only. This is governed by the setting of the Switch Distribution Mode to Local Edit Only on CLI Change parameter in System Preferences. Refer to the *5620 SAM System Administrator Guide* and *5620 SAM Parameter Guide* for more information on the use of this parameter.

1 Choose Policies→*Policy Type* from the 5620 SAM main menu, where *Policy Type* is the type of policy that you want to distribute. The appropriate policies manager form opens.

2 Choose Global from the Policy scope drop-down menu.

3 Click on the Search button.

4 Select the policy that you want to release or distribute.

5 Perform one of the following:

a If the selected policy is in the Draft Configuration Mode, go to step 6.

b If the selected policy is in the Released Configuration Mode, go to step 10.

6 When the selected policy is in the Draft Configuration Mode, the Distribute button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution by performing one of the following:

a To release the selected policy from the policies manager form, click on the Release button. The Release form opens. Go to step 16.

b To release the selected policy from its own Global (Edit) form, click on the Properties button. The *Policy_Type* Global (Edit) form opens. Go to step 7.

7 On the General tab, click on the Switch Mode button beside the Configuration Mode field. A dialog box appears.

8 Click on the Yes button. The policy Configuration Mode changes to Released and the Release form opens automatically.

9 Go to step 16.

10 When the selected policy has previously been released (it is in the Released Configuration Mode) and you want to redistribute it, perform one of the following:

a To distribute the selected policy (without editing it) from the policies manager form, click on the Distribute button. The Distribute form opens. Go to step 16.

b To distribute the selected policy from its own Global (Edit) form, click on the Properties button. The *Policy_Type* Global (Edit) form opens. Go to step 11.

11 View aspects of the global policy, if required.



Note — If you change any parameters in the global policy, the Configuration Mode changes back to Draft. You will need to re-release the policy to the required NEs before it can be distributed to the NEs. Refer to Procedure 42-4 for more information.

12 View, edit, or delete any local definitions of the policy, if necessary, by clicking on the Local Definitions tab. Perform one of the following:

a Double-click on a local policy in the list to view or edit it.

b Click on the Delete button to remove the local definition.

13 Close the local policy form.

14 Click on the Distribute button. If the Distribute button is not visible, click on the More Actions button and choose Distribute. The Distribute form opens.

The Network Elements (Network) option from the drop-down menu is displayed by default.

15 Perform one of the following:

a If you want to select individual NEs for the distribution, go to step 16.

b If you want to use a policy distribution group for the distribution, go to step 18.

16 Select the NEs for release/distribution by moving the appropriate row entries between the Available Objects and Selected Objects panels, as required. Observe the following behavior:

- If the global policy was not previously released/distributed, the Available Objects panel will be populated with a list of compatible NEs to which the global policy can be released/distributed.
- If the global policy was previously released/distributed and you subsequently edit it, the Configuration Mode reverts to Draft. When you switch the Configuration Mode to Released, the Release form opens and displays one of the following:
  - When local definitions exist, the list of NEs to which the policy has already been released and that have their Distribution Mode set to Sync with Global will appear in the Selected Objects panel. These are ready for distribution.
  - When no local definitions exist, all NEs that are eligible to release the policy will appear in the Available Objects panel. These must be moved to the Selected Objects panel for distribution, as required.
- If the global policy was previously released/distributed and you are redistributing it to a new set of NEs (without editing it), the Available Objects panel is populated with a list of NEs. The Local Policy Exists column indicates whether or not local definitions of the policy already exist on the displayed NEs.



Note 1 — The Available Objects and Selected Objects panels both contain a column titled Local Policy Exists. This indicates whether or not local definitions of the policy already exist on the eligible NEs.

Note 2 — On the Distribute form, you can filter the displayed NEs in the Available Objects panel. Click the Available Objects drop-down menu item to choose one of: All NEs, only those containing a local definition of the policy (Local Policy Exists), or only those containing no local definition of the policy (No Local Policy).

Note 3 — You can alternatively choose to use a Policy Distribute Group to distribute the policy. However, you cannot use a Policy Distribute Group and then add further individual NEs to the Selected Objects panel. Refer to Procedure 42-3 for more information on Policy Distribute Groups.

Note 4 — You can click on the Filter icon to open an advanced filter form that allows you to further refine any applicable conditions to use when listing the nodes. Refer to chapter 3 for information on configuring advanced filter searches. The advanced filter can be cleared by choosing the No Filter option in the filter drop-down menu.

17 Go to step 19.

18 Select the Policy Distribute Group option from the drop-down menu and click on the Search button. The available Policy Distribute Groups are displayed in the list.

19 When you select one or more rows in the Available Objects panel, click on the right-pointing arrow button. The chosen object(s) moves to the Selected Objects panel and is ready for distribution. You can also move a row under the Selected Objects panel back to the Available Objects panel by selecting the row and clicking on the left-pointing arrow button. This will exclude it from distribution.

20 Click on the Distribute button to distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. The policy is distributed to the site or sites.

If you are using a Policy Distribute Group for the distribution, once you click the Distribute button, the individual NEs contained in the group are listed in the Available Objects panel. This allows you to monitor the distribution progress for any specific NE.

A progress bar at the lower right of the GUI displays the overall percentage of distribution progress completion to the selected sites. Distribution states (In Progress, Succeeded, or Failed) for individual sites are shown in the Status column for the Selected Objects.



Note — Distribution failures are reported in a pop-up message. You can view the error message to determine the cause of the failure and which NE or NEs were affected. Distribution failures are also reported using JMS.

21 Close the Release/Distribute form. The policy manager form reappears.

22 View the devices to which a policy is distributed, if required.

i Choose the policy.

ii Click on the Properties button. The policy configuration form opens, with the General tab displayed.

iii Click on the Local Definitions tab to view a list of NEs to which the chosen policy has been distributed.

23 Configure the Distribution Mode of the local definitions, if required, by performing the following:

i Click on the Switch Distribution Mode button. If the Switch Distribution Mode button is not visible, click on the More Actions button and choose Switch Distribution Mode. The Switch Distribution Mode - *Policy* form opens.

ii Choose Sync With Global, Local Edit Only, or All from the Distribution Mode parameter drop-down menu. The sites that are configured with the selected distribution mode are listed.

iii Choose one or more NEs from the Available Nodes with Local Policies list.

iv Click on the right-pointing arrow button. The chosen NE(s) moves to the Selected Nodes with Local Policies panel of the form.

v Depending on the distribution mode of the chosen site or sites, perform one of the following steps:

- Click on the Sync With Global button.
- Click on the Local Edit Only button.

vi Close the Switch Distribution Mode - *Policy* form. The policy manager form reappears.

24 To distribute additional policies, perform steps 4 to 23.

Procedure 42-2 To distribute multiple policies

Use this procedure to distribute a group of policies in one action. The policies must all be of the same type. When you distribute a group of global policies, the same conditions and restrictions that apply to the distribution of a single policy exist. Refer to Procedure 42-1 for more information. Additional considerations for multiple policy distribution are provided here.



Note — When you distribute a group of global policies:

- You can set a limit to the maximum number of tasks involved in the bulk policy distribution. Perform Procedure 42-14 to set this limit.
- The default behavior when you release a policy for distribution is that the Distribute window opens and allows you to select the NEs required for distribution. Alternatively, you can enable a parameter setting in the System Preferences that will upon release of the global policy, automatically distribute it to NEs that already have local versions of the policy. Refer to the *5620 SAM System Administrator Guide* and *5620 SAM Parameter Guide* for more information on the use of the Auto Distribute Global Policy when Released parameter.
- Local NE versions of policies that use the Sync With Global distribution mode will allow the NE to receive the distribution of a global policy. However, local NE versions of policies that use the Local Edit Only distribution mode will not allow the NE to receive the global policy. You must ensure that the policy distribution mode for the local policy is set to Sync With Global if you want the NE to receive the global policy distribution.
- Multiple distribution is currently not supported for routing or firewall policies.

1 Choose Policies→*Policy Type* from the 5620 SAM main menu, where *Policy Type* is the type of policy that you want to distribute. The appropriate policies manager form opens.

2 Choose Global from the Policy scope drop-down menu.

3 Click on the Search button.

4 Select the policies that you want to release or distribute.



Note — If you select a combination of policies that are in Draft and Release mode, the Release and Distribute button will be disabled. The policies you select must be in one mode or the other.

5 Perform one of the following:

a If the selected policies are in the Draft Configuration Mode, go to step 6.

b If the selected policies are in the Released Configuration Mode, go to step 7.

6 When the selected policies are in the Draft Configuration Mode, the Distribute button is disabled and the policies cannot be distributed to the NEs. You must first release the policies for distribution. Click on the Release button. The Release form opens. Go to step 9.

7 When the selected policies have previously been released (they are in the Released Configuration Mode) and you want to redistribute them, then click on the Distribute button. The Distribute form opens. The Network Elements (Network) option from the drop-down menu is displayed by default.

8 Perform one of the following:

a If you want to select individual NEs for the distribution, then go to step 9.

b If you want to use a policy distribution group for the distribution, then go to step 11.

9 Select the NEs to release/distribute the policies to and click on the right-pointing arrow button. This moves the required row entries between the Available Objects and Selected Objects panels. Conversely, you can also move a row under the Selected Objects panel back to the Available Objects panel by selecting the row and clicking on the left-pointing arrow button. This will exclude it from distribution. Observe the following behavior:

- The Available Objects panel is populated with a list of compatible NEs to which all the selected policies can be released/distributed.
- When local definitions exist, the list of NEs to which the policies have already been released and that have their Distribution Mode set to Sync with Global will appear in the Selected Objects panel. These are ready for distribution.

10 Go to step 12.

11 Select the Policy Distribute Group option from the drop-down menu and click the Search button. The available Policy Distribute Groups are displayed in the list.



Note — You cannot use a Policy Distribute Group and then add further individual NEs. Refer to Procedure 42-3 for more information on Policy Distribute Groups.

12 Click on the Distribute button to distribute the global policies to the selected devices.

If you are using a Policy Distribute Group for the distribution, once you click the Distribute button, the individual NEs contained in the group are listed in the Available Objects panel. This allows you to monitor the distribution progress for any specific NE.

A progress bar at the lower right of the GUI displays the overall percentage of distribution progress completion to the selected sites. Distribution states (In Progress, Succeeded, or Failed) for individual sites are shown in the Status column for the Selected Objects.



Note — Distribution failures are reported in a pop-up message. You can view the error message to determine the cause of the failure and which NE or NEs were affected. Distribution failures are also reported using JMS.

13 Close the Release/Distribute form. The policy manager form reappears.

14 Close the policy manager form.

Procedure 42-3 To create a policy distribution group

You can create a Policy Distribute Group to specify a group of NEs to distribute a policy to.

1 Choose Policies→ Policy Distribute Group from the 5620 SAM main menu.

The Policy Distribute Group form opens.

2 Click on the Create button. The Policy Distribute Group (Create) form opens, with the General tab displayed.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Group Name
- Description

4 Click on the Network Elements tab.

5 Click on the Add button. The Select Network Elements form opens.

6 Select the NEs that you want to include in the distribution group and click OK. The Select Network Elements form closes and the selected NEs appear in the Network Elements tab list.

7 Repeat steps 5 and 6 to add more NEs to the group, as required.

8 Click the OK button. The Policy Distribute Group (Create) form closes.

Procedure 42-4 To modify a policy

Use this procedure to change existing policies and entries within policies using the 5620 SAM client GUI. Alternatively, you can use the CLI.

When you modify policy match criteria, for example, the IP match criteria for an access ingress policy, click on the Refresh button to ensure that the 5620 SAM client GUI displays the latest set of match criteria.

1 Choose Policies→*Policy Type* from the 5620 SAM main menu, where *Policy Type* is the type of policy that you want to edit.

The Manage *Policy Type* form opens.

2 Choose Global from the Policy scope drop-down menu.

3 Click on the Search button. A list of search results is displayed on the form.

4 Choose the policy that you want to edit.

5 Click on the Properties button. The policy configuration form opens.

6 Perform one of the following:

a If the configuration mode of the policy is set to Released, go to step 7

b If the configuration mode of the policy is set to Draft, configure the parameters, as required, and go to step 13.

7 Configure the parameters, if required. When you modify the configuration, the 5620 SAM changes the Configuration Mode of the policy to Draft.

8 When you modify filter entries for policies with filters, click on the appropriate tab and click on the Refresh button to list the filter entries.

9 Click on the Apply button. A dialog box appears.

10 Click on the Yes button.

11 Perform one of the following steps:

a Compare the global policy with the existing local definitions to verify whether you need to reset the policy configuration to the previously released global policy configuration. Perform steps 8 to 10 of Procedure 42-12.

b Go to step 12.

12 Perform one of the following steps:

a Click on the Action button and choose Reset to Released to reset the global policy configuration to the last released configuration of the policy and to cancel any modifications you entered in step 7. Go to step 18.

b Go to step 13.

13 Click on the Switch Mode button beside the Configuration Mode parameter. A dialog box appears.

14 Click on the Yes button. The policy configuration mode changes to Released and the Release form opens.

15 The NEs that have a local definition of the policy set to Sync with Global are shown in the Selected Objects panel and are ready for distribution. You can select an NE and move it to the Available Objects panel by using the left-pointing arrow. This will exclude it from distribution.

16 Click on the Distribute button to distribute the policy locally to the devices listed in the Selected Objects panel. If the Distribute button is not visible, click on the More Actions button and choose Distribute. The policy is distributed to the site or sites.

A progress bar at the lower right of the GUI displays the overall percentage of distribution progress completion to the selected sites. Distribution states (In Progress, Succeeded, or Failed) for individual sites are shown in the Status column for the Selected Objects.



Note — Distribution failures are reported in a pop-up message. You can view the error message to determine the cause of the failure and which NE or NEs were affected. Distribution failures are also reported using JMS.

17 Close the Release form. The policy manager form reappears.

18 Click on the Local Definitions tab to view the local instances of the global policy, if required.

19 Click on the OK button. A dialog box appears.

20 Click on the Yes button. The policy configuration form closes and the policy manager form reappears.

21 Close the policy manager form.

Procedure 42-5 To delete a policy

Each service SAP and network interface is associated, by default, with the appropriate ingress, egress, or network policy (ID 1). You can replace the default policy with a customer-configured policy, but you cannot entirely remove a QoS policy. When you remove a QoS policy from a SAP or IP interface, the policy association reverts to the default policy (ingress or egress policy ID 1). The default policy cannot be deleted.

A QoS, ACL, or an AA transit IP policy cannot be deleted until it is removed from the all SAPs or network ports where it is applied. When a policy is deleted, it is removed from the 5620 SAM, including the database and all devices.

Do not delete a routing policy from an NE that is associated with one or more services. Multiple services on the NE may use the policy.

1 Choose Policies→*Policy Type* from the 5620 SAM main menu, where *Policy Type* is the type of policy that you want to delete.

The Manage *Policy Type* form opens.

2 Choose Local or Global from the Policy scope drop-down menu. When you set it to Local, you can specify the Local Node IP Address parameter and choose a device by using the Select button and selecting a device in the list.

3 Click on the Search button. A list of search results is displayed in the bottom panel of the form.

4 Choose the policy that you want to delete.

5 Click on the Delete button. A dialog box appears.

6 Click on the Yes button. The policy configuration form closes and the policy manager form reappears. The policy is removed from the policy list.

Procedure 42-6 To copy or overwrite a policy

You can copy an existing QoS policy, rename the policy with a new QoS policy ID, or overwrite an existing policy ID.

1 Choose Policies→*QoS*→*Policy Type* from the 5620 SAM main menu, where *Policy Type* is the type of policy that you want to copy or overwrite.

The Manage *Policy Type* form opens.

2 Choose Local or Global from the Policy scope drop-down menu. When you set it to Local, you can specify the Local Node IP Address parameter and choose a device by using the Select button and selecting a device in the list.

3 Click on the Search button. A list of search results is displayed.

4 Choose the policy that you want to copy or overwrite.

5 Click on the Properties button. The Policy Type (Edit) form opens.

6 Click on the Action button and choose Copy. The Policy Type (Create) form opens.

7 Configure the parameters as required.

8 Click on the Ok button. The Policy Type (Create) form closes and the Policy Type (Edit) reappears.

9 Close the Policy Type (Edit) form. The Manage *Policy Type* form reappears. The new policy is displayed in the list.

10 Close the Manage *Policy Type* form.

Procedure 42-7 To synchronize a policy

You can use the synchronize function to specify the local policy entry as global and redistribute it across all deployed associations. For example, if a policy is distributed to a wide range of devices and on one of these devices the policy was changed, you can use the synchronize command to synchronize the policy on the device and on the 5620 SAM. You must then distribute the policy to all participating devices, as described in Procedure 42-1.



Note — When you synchronize a policy that is in draft mode, the policy is not distributed to existing local definitions. When you synchronize a policy that is in released mode, the 5620 SAM sets the policy to draft mode. You must set the Configuration Mode parameter to Released to distribute the policy to existing local definitions. Only local policies that have the Distribution Mode parameter set to Sync With Global are affected.

1 Choose Policies→*Policy Type* from the 5620 SAM main menu, where *Policy Type* is the type of policy that you want to synchronize.

The Manage *Policy Type* form opens.

2 Choose Local or Global from the Policy scope drop-down menu. When you set it to Local, you can specify the Local Node IP Address parameter and choose a device by using the Select button and selecting a device in the list.

3 Click on the Search button. A list of search results is displayed.

4 Choose the policy or policies that you want to synchronize.

5 Click on the Synchronize button. The Synchronize form opens and the chosen policy appears in the Destination Policy Instance(s) panel at the top.

6 Choose the NE to which the policy is to be synchronized from the Available Local Policies list.

7 Click on the right-pointing arrow button. The chosen NE moves to the Selected Source Local Policy panel of the form.

8 Click on the Synchronize button.

9 Close the Synchronize form.

Procedure 42-8 To perform a policy audit for policy groups and types

An audit compares all local policies with the associated global policies. A policy audit can be performed on all NEs in the network, or limited to a specific NE or group of NEs. All NEs are included in the audit unless they are explicitly chosen. A policy audit can be performed on policy groups and policy types. A policy audit cannot be started when another policy audit is in progress.



Caution — If policy types, global policies are not specified, all policies for which the user has licensing permissions are included in the policy audit.

If NEs are not specified, all NEs that are in the user's span of control are included in the policy audit.

Performing a policy audit may take one or more hours to complete.



Note — Validation is performed to prevent policies from being audited if licensing and span of control prohibits.

If a user performs an audit on objects that are not within their span of control, or they do not have licensing permissions, the audit is aborted and a error message opens. The error message indicates which objects are prohibited.

1 Choose Tools→Policies Audit from the 5620 SAM main menu. The Policy Audit - audit status (Edit) form opens with the General tab displayed.

2 Configure the parameters:

- Include Non Applicable Attributes
- Set to "Local Edit Only" upon finding of differences
- Set to "Sync with Global" upon finding of no differences



Note — The Set to "Local Edit Only" upon finding of differences and Set to "Sync with Global" upon finding of no differences parameters are configurable when the Include Non Applicable Attributes parameter is not enabled.

3 Perform one of the following steps:

a To choose policy groups and policy types to be included in the audit, go to 4.

b If all policy groups and policy types are included in the audit, go to step 10 to set which NEs to include in the audit.

c If all policy groups and policy types and the entire network is included in the audit, go to step 11.

4 Click on the Policy Group Selection tab.

5 Right-click on the Policy Audit icon and choose Select Policy Groups from the contextual menu. The Select Policy Groups form opens.

6 Select policy groups as required and click on the OK button. The chosen policy group keys appear below the Policy Audit icon.

7 Perform one of the following steps:

a If all policy types within the selected groups are included in the audit, go to step 10.

b To choose which policy types within the selected groups are included in the audit, go to step 8.

8 Right-click on a policy group icon and choose Select Policy types from the contextual menu. The Select Policy types - Policy Audit form opens.

9 Select policy types as required and click on the OK button. The chosen policy type icons appear below the Policy Audit icon.

10 Select NEs to include in the audit, if required.

i Click on the Network Element Selection tab to select an NE, or group of NEs to be audit.

ii Click on the Add button. The Select Site form opens.

iii Click on the Search button. A list of NEs is displayed.

iv Click on the NEs to be included in the audit.

v Click on the OK button. The Policy Audit *audit_status* (Edit) form refreshes to display a list of NEs.

11 Click on the Start Audit button.

To interrupt the audit while it is in progress, click on the Stop Audit button.

12 Close the Policy Audit form after the audit finishes.

13 A discrepancy between a global policy and a local instance of the policy generates an alarm. Monitor the dynamic alarm form to view alarms that are generated as a result of the policy audit.



Note — The distribution mode of a local policy may change depending on the parameters set in step 2.

14 Double-click on the alarm in the alarm form. The Alarm Info form opens.

15 Click on the View Alarmed Object button. The Global Policy (Edit) form opens.

16 Perform steps 8 to 11 of Procedure 42-12 to locate the discrepancies between the local and global policies.

17 Close the local and global *Policy_type* (Edit) forms.

Procedure 42-9 To perform a policy audit for multiple global policies with same type

An audit compares all local policies with the associated global policies. A policy audit can be performed on all NEs in the network, or limited to a specific NE or group of NEs. All NEs are included in the audit unless they are explicitly chosen. A policy audit can be performed on one or multiple global policies with the same type. A policy audit cannot be started when another policy audit is in progress.



Caution — If NEs are not specified, all NEs that are in the user's span of control are included in the policy audit.



Note — Validation is performed to prevent policies from being audited if licensing and span of control prohibits.

If a user performs an audit on objects that are not within their span of control, or they do not have licensing permissions, the audit is aborted and a error message opens. The error message indicates which objects are prohibited.

1 Choose Policies→ *Policy_Type* from the 5620 SAM main menu, where *Policy_Type* is the type of policy that you want to audit. The appropriate policies manager form opens.

2 Click on the Search button. A list of policies is displayed.

3 Choose one or multiple policies in the list.

4 Click on the Policy Audit button. A Policy Audit (Edit) form opens with the Global Policy Selection tab displayed and the selected policies listed.

5 Click on the Add button. The Select Policies form opens, displaying a list of global policies to be audited.

6 Select a policy or multiple policies in the list.

7 Click on the OK button. The Policy Audit (Edit) form is refreshed with the selected policies.

8 Click on the General tab.

9 Configure the parameters:

- Include Non Applicable Attributes
- Set to "Local Edit Only" upon finding of differences
- Set to "Sync with Global" upon finding of no differences



Note — The Set to "Local Edit Only" upon finding of differences and Set to "Sync with Global" upon finding of no differences parameters are configurable when the Include Non Applicable Attributes parameter is not enabled.

10 Perform one of the following:

a To audit selected global policies on the entire network, go to step 12.

b To audit selected global policies on selected NEs go to step 11.

11 Select NEs to include in the audit, if required.

i Click on the Network Element Selection tab to select an NE, or group of NEs to be audit.

ii Click on the Add button. The Select Site form opens.

iii Click on the Search button. A list of NEs is displayed.

iv Click on the NEs to be included in the audit.

v Click on the OK button. The Policy Audit (Edit) form refreshes to display a list of NEs.

12 Click on the Start Audit button to proceed with the policy audit.

To interrupt the audit while it is in progress, click on the Stop Audit button.

13 A discrepancy between a global policy and a local instance of the policy generates an alarm. Monitor the dynamic alarm window to view alarms that are generated as a result of the policy audit.

14 Double-click on the alarm in the alarm window. The Alarm Info form opens.

15 Click on the View Alarmed Object button. The Global Policy (Edit) form opens.

16 Perform steps 8 to 11 of Procedure 42-12 to locate the discrepancies between the local and global policies.

17 Close the local and global *Policy_type* (Edit) forms.

Procedure 42-10 To perform a policy audit for global policy

An audit compares all local policies with the associated global policy. A policy audit can be performed on all NEs in the network, or limited to a specific NE or group of NEs. All NEs are included in the audit unless they are explicitly chosen. A policy audit cannot be started when another policy audit is in progress.



Caution — If NEs are not specified, all NEs that are in the user's span of control are included in the policy audit.



Note — Validation is performed to prevent policies from being audited if licensing and span of control prohibits.

If a user performs an audit on objects that are not within their span of control, or they do not have licensing permissions, the audit is aborted and a error message opens. The error message indicates which objects are prohibited.

1 Choose Policies→ *Policy_Type* from the 5620 SAM main menu, where *Policy_Type* is the type of policy that you want to audit. The appropriate policies manager form opens.

2 Click on the Search button. A list of policies is displayed.

3 Select a policy in the list.

4 Click on the Properties button. The *Policy_Name* Global Policy (Edit) form opens.

5 Click on the Local Definitions tab. A list of local policies is displayed.

6 Perform one of the following:

a To audit a specific local policy or a group of local policies, go to step 7.

b If all local policies in the list are included in the audit, go to step 8.

7 Select one or multiple local policies that you want to include in the audit.

8 Click on the Policy Audit button. A Policy Audit (Edit) form opens with the Network Element Selection tab displayed and a list of NEs corresponding to the selected local policies.

9 Click on the General tab.

10 Configure the parameters:

- Include Non Applicable Attributes
- Set to “Local Edit Only” upon finding of differences
- Set to “Sync with Global” upon finding of no differences



Note — The Set to “Local Edit Only” upon finding of differences and Set to “Sync with Global” upon finding of no differences parameters are configurable when the Include Non Applicable Attributes parameter is not enabled.

11 Click on the Start Audit button. To interrupt the audit while it is in progress, click on the Stop Audit button.

12 A discrepancy between a global policy and a local instance of the policy generates an alarm. Monitor the dynamic alarm window to view alarms that are generated as a result of the policy audit.

13 Double-click on the alarm in the alarm window. The Alarm Info form opens.

14 Click on the View Alarmed Object button. The Global Policy (Edit) form opens.

15 Perform steps 8 to 11 of Procedure 42-12 to locate the discrepancies between the local and global policies.

16 Close Global Policy *Policy_type* (Edit) form.

Procedure 42-11 To configure a policy audit schedule

Perform this procedure to configure a schedule to perform regular audits on selected policies and NEs.

An audit compares all local policies with the associated global policy. A policy audit can be performed on all NEs in the network, or limited to a specific NE or group of NEs. All NEs are included in the audit unless they are explicitly chosen. A policy audit cannot be started when another policy audit is in progress.



Caution — If NEs are not specified, all NEs that are in the user's span of control are included in the policy audit.



Note 1 — Validation is performed to prevent policies from being audited if licensing and span of control prohibits.

If a user performs an audit on objects that are not within their span of control, or they do not have licensing permissions, the audit is aborted and a error message opens. The error message indicates which objects are prohibited.

Note 2 — You can configure the maximum number of scheduled audits that are stored for a local policy by setting the Max Number Of Audit Result stored per Local Policy parameter in the System Preferences. Refer to the *5620 SAM System Administrator Guide* for more information.

1 Choose Tools→Policies Audit from the 5620 SAM main menu. The Policy Audit (Edit) form opens, with the General tab displayed.

2 Configure the parameters:

- Include Non Applicable Attributes
- Set to "Local Edit Only" upon finding of differences
- Set to "Sync with Global" upon finding of no differences



Note — The Set to "Local Edit Only" upon finding of differences and Set to "Sync with Global" upon finding of no differences parameters are configurable when the Include Non Applicable Attributes parameter is not enabled.

3 Click on the Schedule Audit button and choose Create from the menu. The Policy Audit Scheduled Tasks (Create) form opens, with the General tab displayed.

4 Configure the parameters:

- Scheduled Task Name
- Scheduled Task Description
- Administrative State

5 Perform one of the following:

a To specify an existing schedule:

i Click on the Select button in the Schedule block. The Select Schedule - Policy Audit Scheduled tasks form opens.

ii Choose a schedule from the list.

iii Click OK. The Select Schedule - Policy Audit Scheduled tasks form closes and the name of the selected schedule appears on the Policy Audit Scheduled Tasks (Create) form.

b To create a new schedule:

i Click on the Select button in the Schedule block. The Select Schedule - Policy Audit Scheduled Tasks form opens.

ii Click the Create button. The SAM Schedule (Create) form opens. Perform steps 3 to 6 of Procedure 7-1 to create the schedule.

6 Click on the Audit tab.

7 Select one or more policy types that you want to include in the audit from the Selected Policies panel.

8 Select one or more NEs that you want to include in the audit from the Selected NEs panel.

9 Click on the Apply button. The Policy Audit Scheduled Tasks (Create) form is updated with the changes.

10 Click the buttons at the bottom of the The Policy Audit Scheduled Tasks (Edit) form to manually Execute and Stop the schedule audit operations, if required.

The User Activity button displays the creation, modification, start and stop operations of the scheduled audit.

11 Once a scheduled policy audit has been completed, you can access the audit results by clicking on the Schedule Audit button in the Policy Audit (Edit) form and choosing View from the menu. The Policy Audit Schedule Tasks list form opens.

12 Select a scheduled task from the list and click the Properties button. The Policy Audit Scheduled Tasks (Edit) form opens.

13 Click on the Audit Scheduled Task Results tab to view a list of results.

14 Select an entry and click Properties to review specific results. The Viewing Old Audit Result indicator lets you know whether you are viewing the latest audit result or not.

15 Close the Policy Audit Scheduled Tasks (Edit) form.

16 Close the Policy Audit Schedule Tasks list form.

17 Close the Policy Audit (Edit) form.

Procedure 42-12 To identify differences between a global and local policy or two local policies



Note — You can cancel the local audit at any time by clicking on the Action button and choosing Local Audit Off on the *Policy_type* (Edit) form.

1 Choose Policies→*Policy_type* from the 5620 SAM main menu, where *Policy_type* is the type of policy that you want to open and search for global and local differences. The Manage *Policy_type* form opens.

2 Choose Local from the Policy scope drop-down menu.

3 Click on the Select button beside the Local Node IP Address parameter. The Select a Network Element form opens.

4 Select a device in the list and click on the OK button. The Select a Network Element form closes and the Manage *Policy_type* form is updated with the NE IP address.

5 Click on the Search button. A list of search results is displayed.

6 Choose the local policy that you want to compare with another policy.

7 Click on the Properties button. The *Policy_type* (Edit) form opens.

8 Click on the Local Audit On button. If the Local Audit On button is not visible, click on the More Actions button and choose Local Audit On. The Local Audit form opens.

9 From the Policy scope drop-down menu:

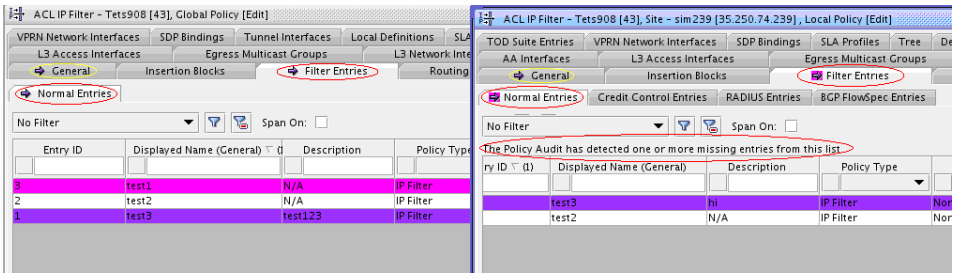
- **a** Choose Global and go to step 10.
- **b** Choose Local and perform the following:
  - **i** Click the Select button to choose an NE. The Select a Network Element form opens.
  - **ii** Select the required NE from the list and click on the OK button. The Select a Network Element form closes and the Local Node IP Address parameter is configured with the address of the selected NE.

10 Click on the OK button. The Local Audit form closes and the appropriate global or local policy opens for comparison, based on your selection in step 9.

11 Perform one of the following steps, as applicable:

a View the differences between the policies by clicking on the tabs that are highlighted with an arrow icon, which indicates that differences exist between the forms. A purple arrow indicates that an attribute is set differently between the two audited forms. A pink arrow indicates that an attribute is missing. A purple arrow in a pink background rectangle indicates that both conditions are occurring. In lists, new entries are highlighted in pink and modified entries are highlighted in purple. Messages are also provided above a list to help isolate the differences on the affected form. The example shown in Figure 42-1 demonstrates some of these various conditions and indications.

Figure 42-1 Policy audit mismatches



Note — Global policies can be distributed to many varying NE types. Local policy audits are performed based on absolute database records. In some cases, this means that when you audit a local policy, a change may be indicated on the associated global policy that does not apply specifically to this local policy. The changed global property may simply not be relevant to the NE associated with this local policy.

For example, a Subscriber Profile global policy contains an HSMDA QoS tab. If a change has been made to a property on this tab in the global policy, but the local policy you are auditing applies to an NE that does not support HSMDA, then the following will occur. When you perform the local audit against the global policy, the global policy form will indicate that there is a difference between the two by displaying an arrow icon on its HSMDA QoS tab. However, since the local policy's NE does not support HSMDA, the local policy form will not even display an HSMDA tab for you to compare with. Any such indicated global changes are irrelevant to the local policy and can be ignored.

b For certain policy types, you can click on a Tree tab on the local or global policy form. New items are highlighted in pink text. Modified items in the tree are highlighted in purple text.

12 Close the local and global *Policy_type* (Edit) forms.

Procedure 42-13 To configure the maximum policy objects per deployer

Perform this procedure to change the default maximum number of NEs to which a policy is distributed to by one deployer. The default value is 10 000 NEs per deployer.



Caution — Contact your Alcatel-Lucent technical support representative before you attempt to modify the nms-server.xml file. Modifying the nms-server.xml file can have serious consequences that can include service disruption.

1 Log in to the 5620 SAM main server station as the samadmin user.

2 Navigate to the 5620 SAM server configuration directory, typically /opt/5620sam/server/nms/config.

3 Create a backup copy of the nms-server.xml file.

4 Open the nms-server.xml file using a plain-text editor.

5 Search for the following XML tag:

```
<policyConfig policyDistributionMaxObjectsPerDeployer="10000"/>
```

6 Change the number, as required. A zero value or a negative number specifies one deployer or all sites, respectively. A one value specifies one deployer per site. The default is 10 000. Alcatel-Lucent recommends that you configure the value between 2000 and 100 000.

If the <numberOfObjectsPerPolicy> is greater than or equal to the <policyDistributionMaxObjectsPerDeployer> one deployer per site is used.

If the <numberOfObjectsPerPolicy> is less than the <policyDistributionMaxObjectsPerDeployer> the maxNumberOfSitesPerDeployer is calculated by policyDistributionMaxObjectsPerDeployer divided by the numberOfObjectsPerPolicy.

7 Save and close the nms-server.xml file.

8 Open a console window.

9 Navigate to the 5620 SAM server binary directory, typically /opt/5620sam/server/nms/bin.

10 If the main server is a standalone server, or the primary server in a redundant deployment, enter the following:

```
bash$ ./nmsserver.bash read_config ↵
```

The main server reads the nms-server.xml file and puts the configuration change into effect.

11 If the main server is the standby server in a redundant deployment, enter the following:

```
bash$ ./nmsserver.bash force_restart ↵
```

The main server restarts and puts the configuration change into effect.

12 Close the console window.

Procedure 42-14 To configure the maximum number of tasks for distribution

The 5620 SAM allows you to select multiple policies of the same type for bulk distribution. Perform this procedure to change the default maximum number of tasks involved when a group of policies is distributed.



Caution — Contact your Alcatel-Lucent technical support representative before you attempt to modify the nms-server.xml file. Modifying the nms-server.xml file can have serious consequences that can include service disruption.

1 Log in to the 5620 SAM main server station as the samadmin user.

2 Navigate to the 5620 SAM server configuration directory, typically /opt/5620sam/server/nms/config.

3 Create a backup copy of the nms-server.xml file.

4 Open the nms-server.xml file using a plain-text editor.

5 Search for the following XML tag:

```
<policyConfig maxTasksForBulkDistribute="200000"/>
```

6 Change the number, as required. The default is 200000. Alcatel-Lucent recommends that you configure the value between 1 and 200000.

7 Save and close the nms-server.xml file.

8 Open a console window.

9 Navigate to the 5620 SAM server binary directory, typically /opt/5620sam/server/nms/bin.

10 If the main server is a standalone server, or the primary server in a redundant deployment, enter the following:

```
bash$ ./nmsserver.bash read_config ↵
```

The main server reads the nms-server.xml file and puts the configuration change into effect.

11 If the main server is the standby server in a redundant deployment, enter the following:

```
bash$ ./nmsserver.bash force_restart ↵
```

The main server restarts and puts the configuration change into effect.

12 Close the console window.

43 — QoS policies

43.1 QoS policies overview *43-2*

43.2 Workflow to configure policer control hierarchy *43-18*

43.3 Workflow to configure 5620 SAM named buffer pools *43-19*

43.4 QoS policies procedures *43-20*

43.1 QoS policies overview

QoS policies define how network traffic is shaped and queued on one or more NEs. You can use the 5620 SAM to create QoS policies that regulate data throughput on the following:

- equipment, for example, ports and MDAs
- routing and forwarding points, for example, access and network interfaces

Access ingress policies

Access ingress policies are applied to access interfaces and specify QoS on ingress.

Access ingress policies define ingress service forwarding class queues and map flows to those queues. When an access ingress policy is created, it always has two queues defined that cannot be deleted: one for the default unicast traffic and one for the default multipoint traffic. These queues exist within the definition of the policy. The queues only get instantiated in hardware when the policy is applied to an access interface. In the case where the service does not have multipoint traffic, the multipoint queue is not instantiated.

In the simplest access ingress policy, all traffic is treated as a single flow and mapped to a single queue, and all flooded traffic is treated with a single multipoint queue.

The required access ingress policy elements include:

- a unique access ingress policy ID
- an exclusive scope for one-time use, or a template scope for use with multiple SAPs and interfaces
- at least one default unicast forwarding class queue
- at least one multipoint forwarding class queue

The optional access ingress policy elements include:

- additional unicast queues up to a total of 8 for each of the 8 forwarding classes
- 8 HSMDA queues that are automatically created when the policy is created; HSMDA queues are only used by HSMDA SAPs
- additional multipoint queues up to 3 per forwarding class for each type of multipoint traffic (broadcast, multicast and destination unknown unicast)
- QoS policy match criteria to map packets to a forwarding class
- A policer to control traffic flow rate.

Each queue can have unique queue parameters to allow individual policing and rate shaping of the flow mapped to the forwarding class. Mapping flows to forwarding classes is controlled by comparing each packet to the match criteria in the policy.

There is one default access ingress policy. The default policy gives all traffic equal priority with the same chance of being sent or dropped during periods of congestion.



Note — The 5620 SAM supports the configuration of HQoS scheduling mechanisms. HQoS provides the ability to rate limit across multiple queues from single or multiple access interfaces for a specific customer. The building blocks for HQoS include access ingress, access egress, and scheduler policies.

See section 61.4 for a sample service configuration using HQoS.

Policy override

You can override some or all settings associated with an access ingress policy on an L2 or L3 access interface, SLA profile, or subscriber profile. See Procedure 43-42. See Procedure 43-43 for information about policy overrides on L2 access interface meters on 7210 SAS NEs. See Procedure 43-44 for information about policy overrides on L2 access interface queues on 7210 SAS-X NEs.



Note — You can override access ingress policies that have the Scope parameter set to template; see Procedure 43-1.

Forwarding classes

The 5620 SAM supports the configuration of eight forwarding classes and class-based queuing or policing on the managed devices. Each forwarding class is only important in relation to other forwarding classes. A forwarding class provides NEs with a method to determine the relative importance of one packet over another packet in a different forwarding class.

Queues are created for a specific forwarding class to determine how the queue output is scheduled into the switch fabric and the type of parameters that the queue accepts. The forwarding class of the packet, and the in-profile and out-of-profile states, determine how the packet is queued and handled at each hop along its path to a destination egress point. Forwarding classes may also be associated with policers instead of queues. Eight forwarding classes are supported. Table 43-1 lists the default definitions for the supported forwarding classes.

Although all forwarding classes support profile marking, it is a good network engineering practise to ensure that all high priority forwarding classes are in-profile (CIR=PIR) and all low priority forwarding classes are out-of-profile (PIR > CIR=0). This way, distinguishing packets as in-profile or out-of-profile only occurs for assured class types.

Table 43-1 Forwarding classes

Forwarding class ID	Forwarding class name	Forwarding class designation	DiffServ name	Class type	Intended
7	Network control	nc	nc2	High priority	For network control traffic
6	High-1	h1	nc1		For a second network control class or delay/jitter sensitive traffic
5	Expedited	ef	ef		For delay/jitter sensitive traffic
4	High-2	h2	h2		For delay/jitter sensitive traffic
3	Low-1	l1	af2	Assured	For assured traffic; default priority for network management traffic
2	Assured	af	af1		For assured traffic
1	Low-2	l2	cs1	Best effort	For best effort traffic
0	be	be			

Forwarding subclasses

You can use forwarding subclasses for additional access ingress packet classification. One or more subclasses can be associated with each forwarding class. The designations for forwarding subclasses are the same as those for the forwarding classes listed in Table 43-1. Each subclass assumes the behavior of its parent forwarding class. and in combination with the forwarding class provides a greater range of access ingress QoS classification possibilities.

Policers

You can add a policer to an access ingress policy to provide traffic flow limiting. Policers are associated with the forwarding classes defined in the access ingress policy. Policers can also be linked to a policer control policy, which maintains a hierarchy of multiple policer objects in the 5620 SAM system. Policers are linked to policer control policies by means of an arbiter. For more information, see "Policer control policies".

Traffic mapping

You can specify the mapping between the ingress traffic and the ingress queue. Mapping is optional and can be based on combinations of customer QoS marking (dot1p, DSCP, EXP, and precedence), and IP criteria, Ipv6 criteria, or MAC criteria. See Table 43-2.

Adding an LspExp rule to a policy forces packets that match the specified MPLS LSP EXP criteria to override the existing forwarding class and enqueuing priority, based on the parameters specified in the LspExp rule. This functionality allows geographically distributed ISP sites to establish site-to-site interconnection service through a backbone network using VPLS/VLL. Each ISP site PE router connects to a 7x50 Ethernet L2 SAP in the backbone network, and traffic is encapsulated in a VPLS/VLL service tunnel. A maximum of eight LspExp rules are allowed on a single access ingress policy.

Table 43-2 Access ingress policy traffic mapping

Tab	Function
Dot1p	Maps the dot1p value of the ingress traffic to the ingress queue ID
DSCP	Maps the DSCP value of the ingress traffic to the ingress queue ID
LspExp	Maps the EXP value of the ingress traffic to the ingress queue ID
Precedence	Maps the precedence value of the ingress traffic to the ingress queue ID
IP Match Criteria	Maps the IP Match Criteria of the ingress traffic to the ingress queue ID
IPv6 Match Criteria	Maps the IPv6 Match Criteria of the ingress traffic to the ingress queue ID
MAC Match Criteria	Maps the MAC Match Criteria of the ingress traffic to the ingress queue ID

Access egress policies

Access egress policies are applied to access egress interfaces and specify QoS on egress.

Access egress policies define egress service queues and map forwarding class flows to queues. In the simplest access egress policy, all forwarding classes are treated like a single flow and mapped to a single queue.

The required access egress policy elements include:

- a unique access egress policy ID
- at least one defined default queue
- an exclusive scope for one-time use, or a template scope for use with multiple SAPs and interfaces

The optional egress policy elements include:

- additional queues up to a total of 8 separate queues for each of the 8 supported forwarding classes
- IEEE 802.1p priority value remarking based on forwarding class
- A policer to control traffic flow rate

Each queue in a policy is associated with one or more of the supported forwarding classes. Each queue can have its individual queue parameters allowing individual rate shaping of the forwarding classes mapped to the queue. More complex service queuing models are supported, where each forwarding class is associated with a dedicated queue.

The forwarding class determination per service egress packet is determined at ingress. If the packet ingresses the service on the same managed device, the service ingress classification rules determine the forwarding class of the packet. If the packet was received over a service tunnel, the forwarding class is marked in the tunnel transport encapsulation.

There is one default access egress policy. The default policy gives all traffic equal priority with the same chance of being sent or dropped during periods of congestion.

Policy override

You can override some or all settings associated with an access egress policy on an L2 or L3 access interface, SLA profile, or subscriber profile. See Procedure 43-42 for more information.



Note — You can override Access Egress policies that have the Scope parameter set to template. See Procedure 43-3 for more information.

Policers

You can add a policer to an access egress policy to provide traffic flow limiting. Policers are associated with the forwarding classes defined in the access ingress policy. Policers can also be linked to a policer control policy, which maintains a hierarchy of multiple policer objects in the 5620 SAM system. Policers are linked to policer control policies by means of an arbiter. For more information, see "Policer control policies".

Traffic mapping

You can specify the mapping between the egress traffic and the egress queue. Mapping is optional and can be based on combinations of customer QoS marking (dot1p, DSCP and precedence), and IP criteria or IPv6 criteria. See Table 43-3.

Table 43-3 Access egress policy traffic mapping

Tab	Function
Dot1p	Maps the dot1p value of the egress traffic to the egress queue ID
DSCP	Maps the DSCP value of the egress traffic to the egress queue ID
Precedence	Maps the precedence value of the egress traffic to the egress queue ID
IP Match Criteria	Maps the IP Match Criteria of the egress traffic to the egress queue ID
IPv6 Match Criteria	Maps the IP Match Criteria of the egress traffic to the egress queue ID

Network policies

Network policies are applied to network interfaces or access uplink ports and specify QoS on egress and ingress.

On ingress, a network policy maps incoming DSCP and EXP values to forwarding class and profile state for traffic received from the core network. On egress, the policy maps forwarding class and profile state to DSCP and EXP values for traffic to be transmitted into the core network.

Network queue policies

Network queue policies are applied to network ports, uplink ports, or daughter cards.

Network queue policies determine:

- the default burst allocations for queues based on the queue's forwarding class
- the CIR, PIR, and burst size parameters for the queue

You cannot use the same network queue policy on devices of different releases. For example, if the 5620 SAM manages a Release 10.0 7750 SR and a Release 11.0 7750 SR, you must create one policy for the Release 10.0 NE and one policy for the Release 11.0 NE.

For network egress, a network burst policy is associated with the network port buffer pool. For network ingress, the network burst policy is associated the network ingress buffer pool of the daughter card.

Network queue policies support multipoint queues and a variable number of forwarding classes. When you want to deploy a network queue policy to devices of different types, you may need to create an instance of the policy for each NE type. Policies that are configured for multipoint queues and a variable number of forwarding classes are deployed only to devices that support the functionality. Modification of an existing policy results in automatic deployment to participating NEs, so must be done with consideration of the policy features and devices involved.

Slope policies

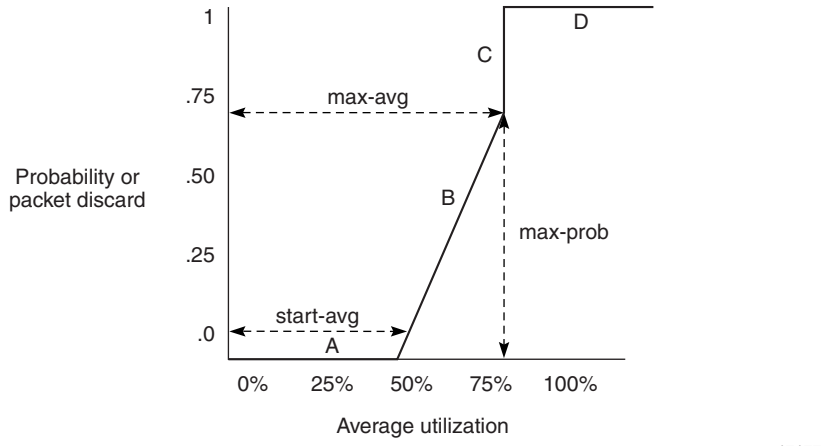
Slope policies are applied to access ports, network ports, and network daughter cards.

Slope policies define weighted RED slope characteristics for buffer pools. Low-priority and high-priority slopes are specified when you configure a slope policy. If a slope policy is not explicitly specified, a default policy is applied.

Each buffer pool supports a high-priority and a low-priority RED slope. The high-priority RED slope manages access to the shared portion of the buffer pool for the high-priority or in-profile packets. The low-priority RED slope manages access to the shared portion of the buffer pool for low-priority or out-of-profile packets. By default, the high-priority and low-priority slopes are disabled.

A RED slope is a graph with an X (horizontal) and Y (vertical) axis. The X axis plots the percentage of shared buffer utilization, from 0 to 100%. The Y axis plots the probability of packet discard marked from 0 to 1. The slope is defined as four sections, as shown in Figure 43-1.

Figure 43-1 RED slope characteristics



Section A is (0, 0) to (start-avg, 0). For this part of the slope, the packet discard value is always zero, which prevents the RED function from discarding packets when the shared buffer average utilization falls between 1 and start-avg.

Section B is (start-avg, 0) to (max-avg, max-prob). This part of the slope is linear where packet discard probability increases from zero to max-prob.

Section C is (max-avg, max-prob) to (max-avg, 1). This part of the slope shows the instantaneous increase of packet discard probability from max-prob to one. A packet discard probability of one results in an automatic discard of the packet.

Section D is (max-avg, 1) to (100%, 1). On this part of the slope, the shared buffer average utilization value of max-avg to 100% results in a packet discard probability of one.

HSMDA slope policies

The HSMDA slope policy controls the management of the HSMDA queue depth. The polices are applied to queues defined in the SAP ingress and SAP egress QoS to provide congestion control. Congestion control includes a defined maximum depth that the queue can reach when packets and RED of congestion and slope-based discards based on queue depth are accepted.

Note — The 5620 SAM does not support HSMDA slope policies on the 7710 SR, 7450 ESS-1, 7750 SR-1, or 7950 XRS.

Shared-queue policies

A shared-queue policy can be applied to daughter cards for optional use by SAPs. The 5620 SAM provides one shared-queue policy for all eight default queues. Each queue is associated with a default forwarding class.

Shared-queue QoS policies can be implemented to facilitate queue consumption on a daughter card; for example, when VPLS, IES, and VPRN services are scaled on one card. Instead of allocating multiple hardware queues for each unicast queue that is defined in an access ingress policy, SAPs with the shared-queuing feature enabled only allocate one hardware queue for each unicast queue.

However, the total amount of traffic throughput at ingress is reduced because ingress packets that are serviced by a shared-queuing SAP are recirculated for additional processing. This can reduce the available bandwidth by half. Shared queuing can also add latency. Network planners should consider these restrictions when they try to scale services on one daughter card.

Table 43-4 lists the queue IDs used by the 5620 SAM to identify the shared-queue types.

Table 43-4 Shared queue types

Shared-queue ID	Shared-queue type
1 to 8	Unicast
9 to 16	Multicast
17 to 25	Broadcast
26 to 32	Unknown



Note — Queue IDs 9 to 32 are also known as multipoint shared queues.

Shared policer output queue

To support hierarchical policing, a default policer-output-queues policy is applied automatically to each IOM that supports ingress policing. In SAM, this shared policer output queue is modeled in the same manner as the existing default shared queue, except that it has only 16 queues.

Multipoint shared-queue policies

Multipoint shared queues minimize the number of multipoint queues that are created for the following:

- ingress VPLS, IES, or VPRN SAPs
- ingress subscriber SLA profiles

Typically, ingress multipoint packets are handled by multipoint queues that are created for each SAP or subscriber SLA profile instance. In some cases, the number of SAPs or SLA profile instances are sufficient for the in-use multipoint queues to represent many thousands of queues on an ingress forwarding plane. If multipoint shared queuing is enabled for the SAPs or SLA profile instances on the forwarding plane, the multipoint queues are not created. Instead, the ingress multipoint packets are handled by the unicast queue that is mapped to the forwarding class of the multipoint packet.

Multipoint shared queues are a superset of shared queuing. With shared queuing on a SAP or SLA profile instance, only unicast packets are processed twice; once for the initial service-level queuing and a second time for switch fabric destination queuing. Shared queuing does not affect multipoint packet handling. Multipoint packet handling in normal service queuing is the same as shared queuing. Shared queuing for unicast packets is automatically enabled when you enable multipoint shared queuing.

The 5620 SAM supports multipoint shared-queue policies for the following services on the 7750 SR, 7450 ESS, 7710 SR:

- Layer 2: VPLS and MVPLS
- Layer 3: IES and VPRN

See the following chapters for more information about enabling multipoint shared queues for a service:

- chapter 68 for VPLS and MVPLS
- chapter 70 for IES
- chapter 71 for VPRN

You can also enable multipoint shared queues in an existing shared-queue policy. See the procedures in this chapter for more information about editing shared-queue policies.

Scheduler policies

Scheduler policies determine the order in which queues are serviced. All ingress and egress queues operate within the context of a scheduler. Multiple queues share the same scheduler. Schedulers control the data transfer between the following queues and destinations:

- service ingress queues to switch fabric destinations
- service egress queues to access egress ports
- network ingress queues to switch fabric destinations
- network egress queues to network egress interfaces

The are two types of scheduler policies:

- single-tier, in which queues are scheduled based on the forwarding class of the queue and the operation state of the queue relative to the queue CIR and PIR
- hierarchical or multi-tier, which allow the creation of a hierarchy of schedules where queues or other schedulers are scheduled by superior schedulers

Scheduler policies are applied to access ingress and access egress interfaces.

Single tier schedulers

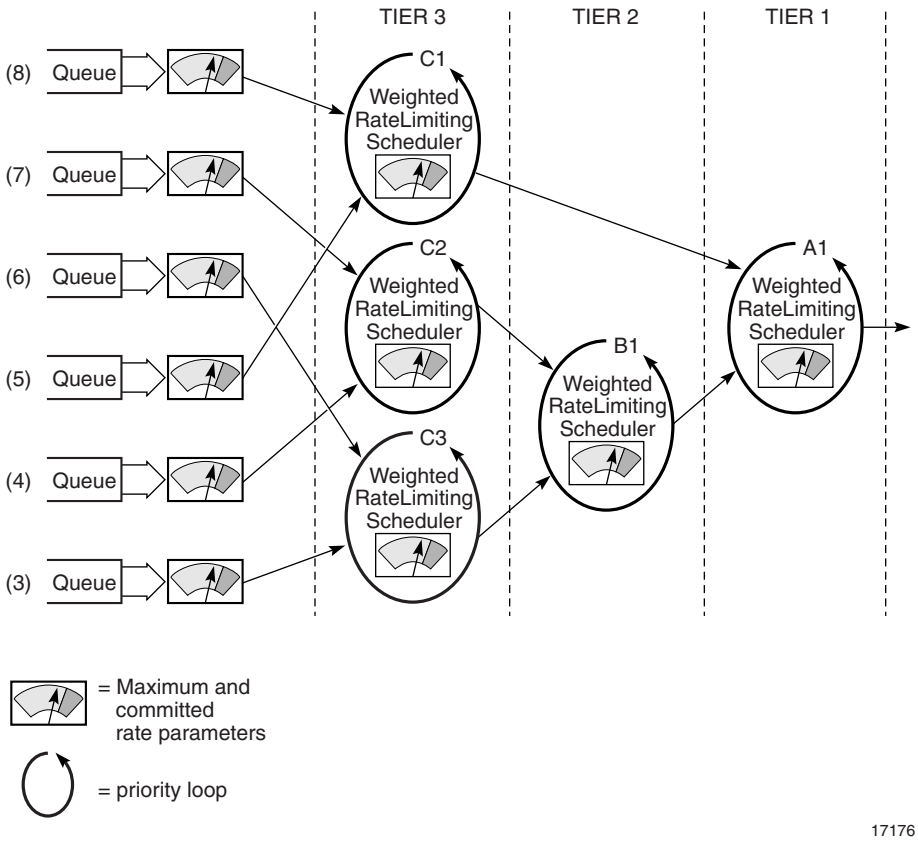
Single-tier scheduling is the default method of scheduling queues. Queues are scheduled with single-tier scheduler policies when no explicit hierarchical scheduler policy is defined or applied. In single-tier scheduling, queues are scheduled based on the forwarding class of the queue and the operational state of the queue relative to the queue CIR and PIR.

Hierarchical schedulers

Hierarchical scheduler policies are used for access ingress and access egress queues. Hierarchical scheduler policies allow you to create a hierarchy of schedulers where queues and other schedulers are scheduled by superior schedulers.

Virtual schedulers are created within the context of a hierarchical scheduler policy. A hierarchical scheduler policy defines the hierarchy and parameters for each scheduler. A scheduler is defined in the context of a tier. The tier level determines the scheduler's position in the hierarchy. Three tiers of virtual schedulers are supported, as shown in Figure 43-2.

Figure 43-2 Hierarchical scheduler and queue association



Tier 1 schedulers are defined without a parent scheduler. A scheduler can enforce a maximum rate of operation for all child queues and associated schedulers.

You can create a tier 2 scheduler without a parent tier 1 scheduler or a tier 3 scheduler without a parent tier 2 scheduler.

Policy override

You can override some or all settings associated with an ingress or egress scheduler policy on an L2 or L3 access interface or subscriber profile. See Procedure 43-42 for more information.

HSMDA scheduler policies

The HSMDA scheduler policy controls the scheduling of a set of HSMDA scheduler classes. The policies are assigned to egress HSMDA ports, and the ingress control scheduler between the HSMDA and ingress forwarding plane. The policies assigned to HSMDA egress ports define how all queues associated with the egress port are scheduled. Scheduler policies assigned to the ingress control scheduler between the HSMDA and ingress forwarding plane define how all ingress queues on the HSMDA, regardless of the ingress port, are scheduled.



Note — The 5620 SAM does not support HSMDA scheduler policies on the 7710 SR, 7450 ESS-1, 7750 SR-1, or 7950 XRS.

Port scheduler policies

Port scheduler policies determine the virtual scheduling of egress ports by allocating HQoS bandwidth based on the available bandwidth at the egress port level. A port scheduler is defined in the context of a tier. The tier level determines the position of the port scheduler in the hierarchy.

The first tier of the scheduling hierarchy manages the total frame bandwidth that the port scheduler allocates to the eight priority levels. The second tier receives bandwidth from the first tier in two priorities—a within-CIR distribution, and an above-CIR distribution. The within-CIR distribution of the second tier provides bandwidth to the third tier within-CIR distributions for each of the eight priority levels. The above-CIR distribution of the second tier provides bandwidth to the above-CIR distribution of the third tier for each of the eight priority levels.

Up to eight groups can be defined within each port scheduler policy. A group has a rate, an optional cir-rate, and inherits the highest scheduling priority of its member levels. In essence, a group receives bandwidth from the port and distributes it within the member levels of the group according to the weight of each level. Each level will compete for bandwidth within the group based on its weight under congestion situation. If there is no congestion, a priority level can achieve up to its rate (cir-rate) worth of bandwidth. One or more levels can map to the same group.



Note — When the agg-rate-limit is applied to queues of a subscriber which are mapped to different priority levels in the same weighted scheduler group, the bandwidth distribution to the queues will be based on the priority of the level.

Orphan queues or schedulers that are not explicitly associated with the port scheduler receive bandwidth after all parented queues and schedulers are allocated bandwidth.

Port scheduler policies are configured on ports and channels.

Policy override

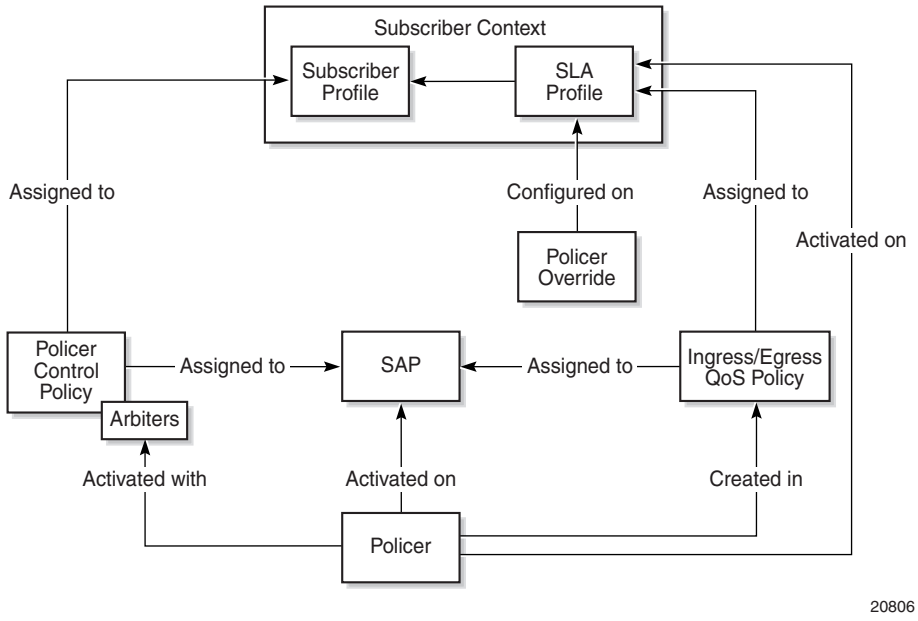
You can override some or all port scheduler settings associated with an access egress queue policy on an L2 or L3 access interface or SLA profile. See Procedure 43-42 for more information.

Policer control policies

Policer control policies allow you to create a control framework, under which policer objects associated with SAPs or subscriber contexts are configured with traffic control parameters. The policer object is applied to the SAP or subscriber context as part of an access ingress policy or access egress policy. The policer control policy is also applied to the SAP or subscriber context. The policer control policy provides the control framework, and policers are associated with the framework by means of arbiters.

When a policer control policy is applied to a SAP or subscriber context, the system creates a parent policer that is bandwidth limited by the policy's maximum bandwidth rate, as defined under the root arbiter. In addition to the root arbiter, the policy may also contain user defined child arbiters that provide bandwidth control for subsets of child policers.

Figure 43-3 Policer association with SAPs and user contexts under policer control hierarchy



A policer is created as part of an access ingress or access egress policy. The policer is configured with a parent arbiter name. When a policy containing a policer is applied to a SAP, the system scans the available arbiters on the SAP. If an arbiter exists with a name that matches the Parent Arbiter parameter on the policer, a policer to arbiter association is established and the policer becomes part of the policer control hierarchy.

In the case of subscriber contexts, the policer control policy is applied to the sub profile used by the subscriber. The system creates a unique policer control hierarchy for each subscriber associated with the sub profile. An access ingress or access egress policy containing a policer is applied to the subscriber SLA profile. The combination of the sub profile and SLA profile at the subscriber level provides the system with the information required to create the policer control hierarchy instance for the subscriber context.

Section 43.2 shows a sample workflow to configure a policer control hierarchy.

Named buffer pool policies

Named buffer pool policy is a QoS policy used to manage named pools. It allows you to create named pools to override the default buffer pool behavior by creating and allocating ingress and egress queues. Named pools are configured in the named buffer pool policy and are applied at the MDA and/or port ingress and egress level.

Named pools can be further defined in Q1 pools configuration. You can configure and assign queue pools to the following policies:

- Access Ingress
- Access Egress
- Network Queue
- Shared Queue

When a policy is associated at the MDA level, named pools defined in the policy allow queues from any port to be associated. When a policy is associated at the port level, named pools are only available to queues associated with that port. A named pool policy that is currently applied to a MDA or port can be deleted after all association between the policy and the MDA or port have been removed.

When buffer pools are created, renamed or deleted, queues mapped to the pools are moved to default pools. When a queue is moved, traffic that was destined for the queue is temporarily moved to a fail over queue. After the old queue is drained, and the new queue is created and associated with the buffer pool, the saved stats are loaded to the new queue and traffic is moved from the fail over queue to the new queue.

Section 43.3 describes a sample workflow to configure Named Buffer Pools and Q1 pools.

Queue Group Template policies

Queue Group Template policies allow you to define the queuing and parenting structure for queue groups on Ethernet ports. The policy defines the number and types of queues within the port queue group, and provides the default queue parameters.

There are two types of Queue Group Template policies: Ingress Queue Group Template policy and Egress Queue Group Template policy.

- Ingress Queue Group Template policies are used for Access Ingress Queue Group creation on Ethernet access ports
- Egress Queue Group Template policies are used for Access Egress Queue Group and Network Egress Queue Group creations on Ethernet ports

Queue Group Template policies are not applicable to L3 interfaces associated with HSMDA ports.

Queue Group Template policies are used in the following network applications:

- Access SAP queue group applications
- Network port queue groups for network interfaces

See chapter 62 for more information about queue groups, the associated network components, and typical applications.

Default policer queue group

The system maintains a special default egress queue group template policy that is applied automatically to all Ethernet ports. The default policer-output-queues policy is configured with two queues:

- Queue 1: configured with a forwarding class value of Best Effort.
- Queue 2: configured with a forwarding class value of Expedite.

All other parameters are default. You cannot delete the default policer-output-queues policy.

7705 SAR fabric profiles

Each daughter card in a 7705 SAR can have two assigned fabric profiles, one for access ingress and one for network ingress. These policies are assigned from the Daughter Card tab of a daughter card slot properties form.

A 7705 SAR fabric profile includes a mode, which cannot be changed after profile creation, and one or more shaping rates. The mode types are Aggregate and Destination. In Aggregate mode, one rate defines the maximum fabric shaping rate that is distributed to each daughter card slot. In Destination mode, there is one fabric shaping rate for each daughter card slot.

In Destination mode, there is also a multi-point shaping rate that is distributed to each daughter card slot.

HSMDA pool policies

The HSMDA pool policy is a QoS policy type that applies to the HSMDA. The policy can be assigned to an ingress or egress HSMDA to control how buffers are distributed between HSMDA queues. HSMDA pool policies do not apply to ports.



Note — The 5620 SAM does not support HSMDA pool policies on the 7710 SR, 7450 ESS-1, 7750 SR-1, or 7950 XRS.

ATM QoS policies

ATM QoS policies are used to specify how ATM traffic is managed by using ATM traffic descriptors, such as service category and shaping. You can create up to 2000 ATM QoS policies per router. ATM QoS policies are applied to access interfaces.

MC MLPPP ingress and egress QoS profiles

MC MLPPP ingress QoS profiles are used to configure the reassembly timeout for each of the four MLPPP classes. You can create up to 128 ingress QoS profiles per NE.

MC MLPPP egress QoS profiles are used to specify queue and queue scheduling parameters for each of the four MLPPP classes.

MCFR ingress and egress QoS profiles

MCFR ingress QoS profiles are used to configure the reassembly timeout for each of the four MLFR classes. You can create up to 128 ingress QoS profiles per NE.

MCFR egress QoS profiles are used to specify queue and queue scheduling parameters for each of the four MLFR classes.

OmniSwitch QoS policies

OmniSwitch QoS provides a way to control traffic flows through the switch based on configured policies. The control may be simple such as allowing or denying traffic, or complicated such as remapping 802.1p bits from a Layer 2 network to ToS values in a Layer 3 network.

The OmniSwitch supports the following types of QoS policies:

- basic QoS—to control traffic prioritization and bandwidth shaping
- ACLs—for Layer 2, 3, and 4 filtering

A QoS policy contains a condition and an action. The condition specifies parameters that the switch checks in incoming traffic flows, such as the destination address or ToS bits. The action specifies what the switch does with traffic that matches the condition; for example, the switch may queue the traffic flow with a higher priority or reset the ToS bits.

Ethernet service policies are used to create UNI and SAP profiles. The profiles are applied to stacked VLAN SAPs and UNIs to control traffic and specify options to manage certain traffic types.

7210 SAS QoS policies

The main types of 7210 SAS QoS policies are:

- QoS policies for classification, defining metering and queuing attributes, and marking
- slope policies that define default buffer allocations and RED slope definitions
- port scheduler policies that determine how queues are scheduled

The 5620 SAM supports the following types of 7210 SAS QoS policies:

- 7210 Access Ingress
- 7210 Port Access Egress
- 7210 SAP Access Egress
- 7210 Network
- 7210 Network Queue
- 7210 Slope
- 7210 Queue Management
- 7210 Port Scheduler
- 7210 Remarking
- 7210 MPLS LSP-Exp Map

Table 43-5 describes the types of 7210 SAS QoS policies.

Table 43-5 7210 SAS QoS policies

Policy type	Applied to	Traffic type affected	Description
7210 Access Ingress	Access port SAP	Ingress	• supports policing using meters or rate shaping (queues) (1) • supports up to eight configurable queues per port (1)
7210 Port Access Egress	Access port SAP	Egress	• defines the SLA for service packets as they egress on the SAP
7210 SAP Access Egress	Access port	Egress	• eight queues per port, each forwarding class mapped to a queue • remarking is always turned on • only supports dot1p remarking
7210 Network	Uplink port, network port, or network interface (2)	Ingress and egress	• only supports ingress rate limiting using meters • eight forwarding classes per port • traffic mapping to forwarding classes based on dot1p, DSCP, or LSP-Exp value markings (3) • supports srTCM, trTCM, trTCM (RFC 2698), and trTCM (RFC 4115)
7210 Network Queue	Uplink port	Egress	• eight hardware queues per port • fixed mapping of forwarding class to queues

(1 of 2)

Policy type	Applied to	Traffic type affected	Description
7210 Slope	Access or uplink port	Egress	• only supports simple RED • low slope drops out-of-profile packets • high slope drops in-profile packets
7210 Queue Management		Egress	• defines slope parameters that determine a WRED profile for each queue
7210 Port Scheduler	Access or uplink port	Egress	• defines scheduling among the queues and the weight proportion for each queue
7210 Remarking	Access or uplink port	Egress	• configures the remarking behavior for the NE at the egress of the access SAPs, ports, and IP interfaces
7210 MPLS LSP-Exp Map	Network interfaces	MPLS packets	• allows separate mappings of profiles and forwarding classes on network interfaces

(2 of 2)

Notes

(1) HQoS access ingress queues are supported only on the 7210 SAS-X, Release 5.0 R4 or later. The system resource profile must be appropriately configured. See "System resource profile" in section 8.5 and Procedure 13-20.

(2) The 7210 SAS-E supports the use of QoS policies on uplink ports. The 7210 SAS-M, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, and 7210 SAS-X 24F 2XFP support the use of QoS policies on network ports and network interfaces.

(3) Dot1p and DSCP apply only to network ports. LSP-Exp applies only to network interfaces.

See the 7210 SAS OS Quality of Service Guides for more information about 7210 SAS QoS and QoS policies.

43.2 Workflow to configure policer control hierarchy

This workflow assumes that the following components already exist:

- a policer control policy
- an access ingress or access egress policy
- a subscriber
- an access interface or SAP

1 Configure arbiters in a policer control policy. See Procedure 43-20 for more information.

i Create arbiters.

ii Configure parent/child relationships between arbiters to build a policer control hierarchy.

2 Configure a policer in an access ingress or access egress policy. See Procedures 43-1 and 43-2 for more information.

   i Create a policer to configure traffic control parameters.

   ii Assign a parent arbiter to the policer to associate it with the hierarchy configured in the policer control policy.

3 Assign the policer control policy to a subscriber that is configured with an access ingress or access egress policy that includes a policer. See Procedure 54-18 for more information.

4 As required, assign the policer control policy to an access interface or SAP that is configured with an access ingress or access egress policy that includes a policer.

   a For an IES L3 access interface, see Procedure 70-17 for more information.

   b For an IES SAP, see Procedure 70-12 for more information.

   c For a VPLS L2 access interface, see Procedure 68-24 for more information.

   d For a VPLS B-L2 access interface, see Procedure 68-66 for more information.

   e For a VPLS I-L2 access interface, see Procedure 68-70 for more information.

   f For a VPRN L3 access interface, see Procedure 71-22 for more information.

   g For a VPRN SAP, see Procedure 71-60 for more information.

43.3 Workflow to configure 5620 SAM named buffer pools

1 Configure a named pool buffer Policy. See Procedure 43-22 for more information.

2 Enable named pool to be configured for a port or MDA. See Procedure 15-28 for more information.

3 Apply a named pool policy to an MDA. See Procedure 15-33 for more information.

4 Apply a named pool policy to a port. See Procedure 16-1 for more information.

5 Configure Q1 pools. See Procedure 43-30 for more information.

6 Assign Q1 pools to access ingress policies. See Procedure 43-1 for more information.

7 Assign Q1 pools to access egress policies. See Procedure 43-3 for more information.

8 Assign Q1 pools to network queue policies. See Procedure 43-12 for more information.

9 Assign Q1 pools to shared queue policies. See Procedure 43-14 for more information.

43.4 QoS policies procedures

This section contains procedures relating to the configuration and maintenance of QoS policies.

Procedure 43-1 To configure an access ingress policy

1 Choose Policies→QoS→SROS QoS→Access Ingress→Access Ingress from the 5620 SAM main menu. The Access Ingress Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Access Ingress Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Auto-Assign ID
- ID
- Displayed Name
- NE Policy Name
- Description
- Scope
- Priority
- MAC Criteria Type
- Default FC

The packets that are received on an ingress SAP using this policy are classified to the specified default forwarding class. See Table 43-1 for more information about forwarding classes.

4 Click on the Queues tab.

The two default queues that cannot be deleted are displayed—the default unicast traffic queue (ID 1) and the default multipoint traffic queue (ID 11).

i Click on the Create button. The Queue form opens with the General tab displayed.

ii Configure the parameters:

- ID
- Displayed Name
- Description
- Pool Name
- Multipoint
- Scheduler button
- Mode
- Expedite



Note 1 — You can use the Select button beside the Pool Name parameter to configure the parameter.

Note 2 — Before you can configure the Pool Name parameter, you must create a Q1 pool using Procedure 43-30.

iii Click on the Select button in the Slope Policy panel to choose a slope policy. The Select Slope Policy search form opens.

iv Select a policy in the list and click on the OK button. The Select Slope Policy form closes and the policy information is displayed on the Queue (Edit) form.

v Click on the Select button in the Advanced Configuration Policy panel to choose a policy. The Select Advanced Configuration Policy search form opens.

vi Select a policy in the list and click on the OK button. The Select Advanced Configuration Policy form closes and the policy name is displayed on the Queue form.

vii Click on the CIR/PIR tab.

viii Configure the parameters:

- Rate Type
- Policed
- CIR (kbps)
- PIR (kbps)
- CIR (%)
- PIR (%)
- CIR Adaptation
- PIR Adaptation

The CIR (kbps) and PIR (kbps) are displayed when the Rate Type is set to kbps. The CIR (%) and PIR (%) parameters are displayed when the Rate Type parameter is not set to kbps.

Ensure that the CIR value is lower than the PIR value.

ix Click on the Burst Size tab.

x Configure the parameters:

- Committed Burst Size (kb)
- Maximum Burst Size (bytes)
- High Priority Reserved
- Burst Limit (kb)

The parameters are configurable when the Default check box above each is deselected.

Ensure that the Committed Burst Size (kb) value is lower than the Maximum Burst Size (bytes) value.

xi Click on the OK button. A dialog box appears.

xii Click on the OK button. The Access Ingress Policy (Create) form reappears.

xiii To configure additional queues, return to step i. You can add up to 32 queues.

5 Click on the Policer tab.

i Click on the Create button. The Access Ingress Policer form opens.

ii On the General tab, configure the parameters:

- ID
- Description
- Parent Arbiter
- Stats Mode
- Packet Byte Offset

iii Click on the Select button in the Advanced Configuration Policy panel to choose a policy. The Select Advanced Configuration Policy search form opens.

iv Select a policy in the list and click on the OK button. The Select Advanced Configuration Policy form closes and the policy name is displayed on the Policer form.

v Click on the CIR/PIR tab and configure the parameters:

- Rate Type
- CIR (kbps)
- PIR (kbps)
- CIR (%)
- PIR (%)
- CIR Adaptation
- PIR Adaptation
- Profile Capped

The CIR (kbps) and PIR (kbps) are displayed when the Rate Type is set to kbps. The CIR (%) and PIR (%) parameters are displayed when the Rate Type parameter is set to Percent Local Limit.

Ensure that the CIR value is lower than the PIR value.

vi Click on the Burst Size tab and configure the parameters:

- Committed Burst Size (kb)
- Maximum Burst Size (bytes)
- High Priority Reserved
- Burst Limit (kb)

vii Click on the OK button to save the changes. A dialog box appears.

viii Click on the OK button. The Access Ingress Policer form closes, and the Access Ingress Policy form reappears.

6 Click on the Forwarding Classes tab. You can create one entry for each of the eight forwarding class types.

i Click on the Create button. The Forwarding Class (Create) form opens with the General tab displayed.

ii Configure the Forwarding Class parameter.

iii Perform any of the following:

- If you need to configure a queue group for some or all traffic types, complete steps iv and v.
- If you need to configure queues for some or all traffic types, complete step v.
- If you need to configure policers for some or all traffic types, complete step vii.

iv On the Traffic Control panel, configure the Use Queue Group parameter for any of the Unicast, Broadcast, Multicast, and Unknown traffic types.

On the Queues panel, click on the Select button beside the Queue Group Template Policy parameter and select a queue group template policy from the Select Queue Group Template Policy form.



Note — If the Use Queue Group parameter is enabled for the global policy, the Queue ID, Multipoint Queue ID, Broadcast Queue ID, and Unknown Queue ID parameters, if selected, are validated against the specified Queue Group Template Policy. The Queue ID is validated against the local queues for each local policy instance.

v On the Queues panel, configure the parameters:

- Queue ID

  The parameter must be set to a unicast ID. Set the parameter to 0 if you want the default queue ID to be used.
- Multipoint Queue ID

  The parameter must be set to a multicast ID. Set the parameter to 0 if you want the default queue ID to be used.
- Broadcast Queue ID

  The parameter must be set to a multicast ID. Set the parameter to 0 if you want the default queue ID to be used.
- Unknown Queue ID

  The parameter must be set to a multicast ID. Set the parameter to 0 if you want the default queue ID to be used.

vi On the Traffic Control panel, configure the Use Policer parameter for any of the Unicast, Broadcast, Multicast, and Unknown traffic types.

vii On the Policers panel, for each traffic type configured with the Use Policer parameter, configure the appropriate Policer ID parameter:

- FP Redirect Group
- Policer ID
- Multipoint FP Redirect Group
- Multipoint Policer ID
- Broadcast FP Redirect Group
- Broadcast Policer ID
- Unknown FP Redirect Group
- Unknown Policer ID

The FP Redirect Group, Multipoint FP Redirect Group, Broadcast FP Redirect Group, and Unknown FP Redirect Group parameters are displayed only when the associated traffic types in the Traffic Control panel are configured to use policers.



Note — Policer IDs created using a 5620 SAM release earlier than 10.0 are displayed only when the associated traffic types in the Traffic Control panel are configured to use policers.

viii Click on the Select button beside each Policer ID parameter and choose a policer from the Select Policer form. The policer must exist in the access ingress policy from step 5.

ix Configure the parameters:

- In Remark
- Out Remark
- In Precedence
- Out Precedence
- In DSCP
- Out DSCP
- Profile
- Mark DE bit 1 as Out of Profile
- Egress Override Forwarding Class

The In Precedence parameter is configurable when the In Remark parameter is set to precedence.

The Out Precedence parameter is configurable when the Out Remark parameter is set to precedence.

The In DSCP parameter is configurable when the In Remark parameter is set to dscp.

The Out DSCP parameter is configurable when the Out Remark parameter is set to dscp.

The Multicast, Broadcast, and Unknown IDs must be set to multicast IDs. The default ID for multicast, broadcast, and unknown queues is 11.

x Click on the Sub Classes tab.

xi Click on the Create button. The Forwarding SubClass form opens.

xii Configure the parameters:

- Displayed Name
- In Remark
- Out Remark
- In Precedence
- Out Precedence
- In DSCP
- Out DSCP
- Profile
- Mark DE bit 1 as Out of Profile
- Egress Override Forwarding Class

The In Precedence parameter is configurable when the In Remark parameter is set to precedence.

The Out Precedence parameter is configurable when the Out Remark parameter is set to precedence.

The In DSCP parameter is configurable when the In Remark parameter is set to dscp.

The Out DSCP parameter is configurable when the Out Remark parameter is set to dscp.

xiii Click on the OK button. A dialog box appears.

xiv Click on the OK button. The Forwarding SubClasses form closes and the Forwarding Class form reappears.

xv Click on the OK button. A dialog box appears.

xvi Click on the OK button. The Forwarding Class (Create) form closes and the Access Ingress Policy form reappears.

7 Click on the Dot1p tab.

i Click on the Create button. The Dot1p form opens.

ii Configure the parameters:

- Dot1p
- Forwarding Class
- Priority

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The Dot1p form closes and the Access Ingress Policy form reappears.

8 Click on the DSCP tab.

i Click on the Create button. The DSCP form opens.

ii Configure the parameters:

- DSCP
- Forwarding Class
- Priority

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The DSCP form closes and the Access Ingress Policy form reappears.

9 Click on the Precedence tab.

i Click on the Create button. The Precedence form opens.

ii Configure the parameters:

- Precedence
- Forwarding Class
- Priority

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The Precedence form closes and the Access Ingress Policy form reappears.

10 Perform one of the following:

a Click on the IP Match Criteria tab to configure IPv4 match criteria.

i Click on the Create button. The IP Match form opens.

ii Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Forwarding Class
- Priority
- Protocol
- Fragment
- Source IP
- Src Mask
- Destination IP
- Dst Mask
- DSCP
- Source Port
- Destination Port

The Source Port and Destination Port parameters appear only when the Protocol parameter value is TCP, UDP, or UDPTCP (*).

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The IP Match form closes and the Access Ingress Policy form reappears.

b Click on the MAC Match Criteria tab.

i Click on the Create button. The MAC Match form opens.

ii Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Forwarding Class
- Priority
- Frame Type
- Source MAC
- Mask
- Destination MAC
- ATM VCI
- Mask
- Dot1p
- Mask
- Inner Tag Value
- Inner Tag VID Mask
- Outer Tag Value
- Outer Tag VID Mask
- DSAP
- DSAP Mask
- SSAP
- SSAP Mask
- SNAP OUI
- SNAP PID
- Ether Type

The Source MAC, Destination MAC, Dot1p, and Mask parameters are configurable when the check box for each parameter is selected.

The Inner Tag Value, Inner Tag VID Mask, Outer Tag Value, and Outer Tag VID Mask parameters are configurable when the MAC Criteria Type parameter is set to VID and the Frame Type parameter is set to Ethernet II.

The DSAP, DSAP Mask, SSAP, and SSAP Mask parameters are configurable when the Frame Type parameter value is e802dot2LLC.

The SNAP OUI and SNAP PID parameters are configurable when the Frame Type parameter value is e802dot2SNAP.

The Ether Type parameter is configurable only when the Frame Type parameter value is Ethernet II.

The ATM VCI parameter is configurable only when the Frame Type parameter value is ATM.

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The MAC Match form closes and the Access Ingress Policy form reappears.

c Click on the IPv6 Match Criteria tab.

i Click on the Create button. The IPv6 Match form opens.

ii Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Forwarding Class
- Priority
- Protocol
- Source IP
- Src Mask
- Destination IP
- Dst Mask
- DSCP
- Source Port
- Destination Port

The Source Port and Destination Port parameters appear only when the Protocol parameter value is TCP, UDP, or UDPTCP (*).

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The IPv6 Match form closes and the Access Ingress Policy form reappears.

11 Click on the Lsp Exp tab.

i Click on the Create button. The Lsp Exp Create form opens.

ii Configure the parameters:

- LspExp
- Forwarding Class
- Priority

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The Lsp Exp Create form closes and the Access Ingress Policy form reappears.

12 Click on the Apply button to save the policy. The Access Ingress Policy form is refreshed with additional buttons.

13 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

14 Close the Access Ingress Policy form. The Access Ingress Policies form reappears.

15 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 43-2 To configure a 7210 SAS or 1830 PSS access ingress policy

1 Choose Policies→QoS→SROS QoS→Access Ingress→7210 and 1830 Access Ingress from the 5620 SAM main menu. The 7210 and 1830 Access Ingress Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy. The SAP Access Ingress, Global Policy (Edit) form opens with the General tab displayed.

b Click on the Create button. The SAP Access Ingress, GlobalPolicy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Scope
- Number Of Qos Classifiers
- Default FC
- Profile
- MAC Match Criteria type
- IP Match Criteria type
- Allow any IPV6 Match
- IPV6 Match Criteria type

The packets that are received on an ingress SAP using this policy are classified to the specified default forwarding class. See Table 43-1 for more information about forwarding classes.

You can only configure the IPV6 Match Criteria type parameter when the Allow any IPV6 Match parameter is set to true.



Note — You cannot configure IPv6 ingress classification for 1830 PSS devices.

4 Click on the Meter tab.

i Click on the Create button. The Meter (Create) form opens with the General tab displayed.

ii Configure the parameters:

- ID
- Rate Mode
- MultiPoint

iii Click on the CIR/PIR tab and configure the parameters.

- CIR Adaptation
- PIR Adaptation
- CIR (kbps)
- PIR (kbps)

iv Click on the Burst Size tab and configure the parameters:

- Committed Burst Size (kbps)
- Maximum Burst Size (kbps)

v Click on the OK button. A dialog box appears.

vi Click on the OK button.

5 Click on the Queues tab.

i Click on the Create button. The AccessIngressQueue, 7210 Access Ingress Policy, Global Policy (Create) form opens.

ii Configure the parameters:

- ID
- Displayed Name
- Description

iii Click on the Select button in the Queue Management Policy panel. The Select Queue Management Policy form opens.

iv Configure the filter criteria, if required, and click on the Search button.

v Choose a queue management policy and click on the OK button. The Select Queue Management Policy form closes.

vi Configure the parameters:

- Port Parent
- Weight
- CIR Level
- CIR (kbps)
- CIR Adaptation
- PIR (kbps)
- PIR Adaptation

vii Click on the OK button. A dialog box appears.

viii Click on the OK button.

ix Repeat steps i to viii to create additional queues, as required. You can create up to eight queues.



Note — You can configure queues anytime, but queues can only be attached to SAPs when the system resource profile for the NE is appropriately configured. See Procedure 13-20.

6 Click on the Forwarding Classes tab.

7 Click on the Create button. The Forwarding Class (Create) form opens. You can create one entry for each of the eight forwarding class types.

8 Configure the Forwarding Classes parameter.

9 Perform one of the following:

a Assign a queue to the forwarding class.

i Configure the Queue ID parameter. Click on the Select button to choose a queue from a list of queues configured in step 5.

ii Click on the OK button. A dialog box appears.

iii Click on the OK button. The Forwarding Classes tab is displayed.

b Assign a meter to the forwarding class.

i Configure the parameters:

- Meter ID
- Multicast Meter ID
- Broadcast Meter ID
- Unknown Meter ID

Click on the Select button to choose a meter from a list of meters configured in step 4.

ii Click on the OK button. A dialog box appears.

iii Click on the OK button. The Forwarding Classes tab is displayed.

10 Repeat steps 7 to 9 to configure additional forwarding classes, as required.



Note — Click on the Relations tab for a graphic view of queue or meter assignments to forwarding classes.

11 Perform one of the following:

a Click on the IP Match Criteria tab.

i Click on the Create button. The IP Match (Create) form opens.

ii Configure the parameters:

- ID
- Displayed Name
- Description
- Forwarding Class
- Protocol
- Profile
- Source IP
- Src Mask
- Destination IP
- Dst Mask
- Source Port
- Port Src
- Destination Port
- Port Dst
- DSCP

You can only configure the Protocol, Source IP, Src Mask, Destination IP and Dst Mask parameters when the IP Match Criteria type parameter is set to Any in step 3.

You can only configure the Source Port, Port Src, Destination Port and Port Dst parameters when the IP Match Criteria type parameter is set to Any in step 3 and the Protocol parameter is set to TCP or UDP.

You can only configure the Source IP, Destination IP, Source Port, Port Src, Destination Port, Port Dst and DSCP parameters when the check box for these parameters is selected.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The IP Match form closes and the SAP Access Ingress, Global Policy form appears.

b Click on the MAC Match Criteria tab.

i Click on the Create button. The MAC Match (Create) form opens.

ii Configure the parameters:

- ID
- Displayed Name
- Description
- Forwarding Class
- Profile
- Source MAC
- Mask
- Destination MAC
- Mask
- Dot1p
- Mask
- Ether Type

You can only configure the Source MAC, Destination MAC, and Ether Type parameters when the MAC Match Criteria type parameter is set to Any in step 3.

You can only configure the Source MAC, Destination MAC, Dot1p, Mask, and Ether Type parameters when the check box for these parameters is selected.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The MAC Match form closes and the SAP Access Ingress, Global Policy form displays.

c Click on the IPv6 Match Criteria tab.



Note — You cannot configure IPv6 ingress classification for 1830 PSS devices.

i Click on the Create button. The IPv6 Match (Create) form opens.

ii Configure the parameters:

- ID
- Displayed Name
- Description
- Forwarding Class
- Profile
- Protocol
- Source IP
- Src Mask
- Destination IP
- Dst Mask
- Source Port
- Port Src
- Destination Port
- Port Dst
- DSCP

You can only configure the Protocol, Source IP, Src Mask, Destination IP and Dst Mask parameters when the IPV6 Match Criteria type parameter is set to Any in step 3.

You can only configure the Source Port, Port Src, Destination Port and Port Dst parameters when the IPV6 Match Criteria type parameter is set to Any in step 3 and the Protocol parameter is set to TCP or UDP.

You can only configure the Source IP, Destination IP, Source Port, Port Src, Destination Port, Port Dst and DSCP parameters when the check box for these parameters is selected.

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The IPv6 Match form closes and the SAP Access Ingress, Global Policy form appears.

12 Click on the Apply button to save the policy. The SAP Access Ingress, Global Policy form appears with additional buttons.

13 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

14 Close the SAP Access Ingress, Global Policy form. The 7210 and 1830 Access Ingress Policies form reappears.

15 Close the 7210 and 1830 Access Ingress Policies form.

Procedure 43-3 To configure a SAP access egress policy

1 Choose Policies→QoS→SROS QoS→Access Egress→SAP Access Egress from the 5620 SAM main menu. The SAP Access Egress Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The SAP Access Egress Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- NE Policy Name
- Ethernet Ctag
- Scope
- Packet Byte Offset
- Low Burst Max Class

4 If you are creating a 7705 SAR MC MLPPP access egress policy, configure the Use As Multiclass MLPPP Policy For 7705 SAR parameter. Otherwise, go to step 8.

5 Click on the Select button in the WRR Policy panel to choose a WRR policy. The Select WRR Policy search form opens.

6 Select a policy in the list and click on the OK button. The Select WRR Policy form closes and the policy information is displayed on the Access Egress Policy form.

7 Click on the Apply button.

8 Click on the HSMDA Queues tab. Eight default queues are displayed on the form.

i Select a queue and click on the Properties button. The Access Egress HSMDA Queue (Create) form opens with the General tab displayed.

ii Modify the parameters, if required:

- Displayed Name
- Description

iii Click on the Select button in the Slope Policy panel to choose a slope policy. The Select Slope Policy search form opens.

iv Select a policy in the list and click on the OK button. The Select Slope Policy form closes and the policy information is displayed on the Access Egress HSMDA Queue (Create) form.

v Click on the PIR/Burst Size tab.

vi Configure the parameters:

- PIR (kbps)
- PIR Adaptation
- Maximum Burst Size (bytes)
- Burst Limit (bytes)

You must deselect the associated MAX check box to configure the PIR (kbps) parameter.

You must deselect the associated Default check box to configure the Maximum Burst Size (bytes) or Burst Limit (bytes) parameter.

vii Click on the OK button. The SAP Access Egress Policy (Create) form reappears.

9 Click on the Queues tab. One default queue is displayed on the form.

i Click on the Create button. The Queue (Create) form opens with the General tab displayed.

ii Configure the parameters:

- ID
- Displayed Name
- Description
- Pool Name
- Expedite
- Port Average Overhead (%)
- Scheduler button
- Level
- Weight
- CIR Level
- CIR Weight
- Port Parent
- Level
- Weight
- CIR Level
- CIR Weight
- Use WRED Queue
- Packet Byte Offset



Note 1 — You can use the Select button beside the Pool Name parameter to configure the parameter.

Note 2 — Before you can configure the Pool Name parameter, you must create a Q1 pool using Procedure 43-30.

The Scheduler button, Level, Weight, CIR Level, and CIR Weight parameters in the Parent Scheduler panel are not configurable when the Port Parent parameter in the Port Parent panel is set to true.

iii Click on the Select button in the Slope Policy panel to choose a slope policy. The Select Slope Policy search form opens.

iv Select a policy in the list and click on the OK button. The Select Slope Policy form closes and the policy information is displayed on the Queue form.

v Click on the Select button in the Advanced Configuration Policy panel to choose a policy. The Select Advanced Configuration Policy search form opens.

vi Select a policy in the list and click on the OK button. The Select Advanced Configuration Policy form closes and the policy name is displayed on the Queue form.

vii Click on the CIR/PIR tab.

viii Configure the parameters:

- Rate Type
- CIR (kbps)
- PIR (kbps)
- CIR (%)
- PIR (%)
- CIR Adaptation
- PIR Adaptation

The CIR (kbps) and PIR (kbps) are displayed when the Rate Type is set to kbps. The CIR (%) and PIR (%) parameters are displayed when the Rate Type parameter is not set to kbps.

ix Click on the Burst Size tab.

x Configure the parameters:

- Committed Burst Size (kb)
- Maximum Burst Size (bytes)
- High Priority Reserved
- Burst Limit (kb)

Ensure that the Committed Burst Size (kb) value is lower than the Maximum Burst Size (bytes) value.

xi Click on the OK button. A dialog box appears.

xii Click on the OK button. The SAP Access Egress Policy (Create) form reappears.

xiii To create additional queues, go to step i. You can create up to eight queues.

10 Click on the Policer tab.

i Click on the Create button. The Access Egress Policer form opens.

ii On the General tab, configure the parameters:

- ID
- Description
- Parent Arbiter
- Stats Mode
- Packet Byte Offset

iii Click on the Select button in the Advanced Configuration Policy panel to choose a policy. The Select Advanced Configuration Policy search form opens.

iv Select a policy in the list and click on the OK button. The Select Advanced Configuration Policy form closes and the policy name is displayed on the Policer form.

v Click on the CIR/PIR tab and configure the parameters:

- Rate Type
- CIR (kbps)
- PIR (kbps)
- CIR (%)
- PIR (%)
- CIR Adaptation
- PIR Adaptation
- Profile Capped

The CIR (kbps) and PIR (kbps) are displayed when the Rate Type is set to kbps. The CIR (%) and PIR (%) parameters are displayed when the Rate Type parameter is set to Percent Local Limit.

vi Click on the Burst Size tab and configure the parameters:

- Committed Burst Size (kb)
- Maximum Burst Size (bytes)
- High Priority Reserved

vii Click on the OK button to save the changes. A dialog box appears.

viii Click on the OK button. The Access Egress Policer form closes, and the SAP Access Ingress Policy form reappears.

11 Click on the Forwarding Classes tab.

i Click on the Create button. The Forwarding Class (Create) form opens.

ii Configure the Forwarding Class parameter.

iii Complete one of the following for each Forwarding Class you create:

- If you need to configure a policer, set the Traffic Control parameter for the Use Policer option and go to step iv.
- If you need to configure a local queue, set the Traffic Control parameter for the Use Queue option and configure the Port Redirect Queue Group parameter as required, then go to step viii.
- If you need to configure a queue from a queue group, set the Traffic Control parameter to the Use Queue Group option and go to step vi.

iv On the Policers panel, configure the Policer ID parameter by clicking on the Select button and choosing a policer from the Select Policer - Forwarding Class - Access Egress Policy list, then click OK.

v Configure the Port Redirect Queue Group parameter as required. If you disable this parameter, then go to step vi. Otherwise go to step viii.

vi In the Queue Group panel, click on the Select button beside the Queue Group Template Policy parameter and choose the required policy from the list, then click OK.

vii Configure the Instance ID parameter.

viii Configure the Queue ID parameter by clicking on the Select button to open the Select Queue - Forwarding Class - Access Egress Policy list form.



Note — You cannot map a Forwarding Class to a non-existent or deleted Queue ID. Use the Select button to choose a Queue ID, as opposed to manually entering it in the Queue ID field.

The queue you can select here is dependent on the Traffic Control parameter setting you chose in step iii, as follows:

- Use Queue: If you specified this setting, then you can only select a locally-defined queue. The local queue in this context is either the default queue or one you created for this policy in step 9. The local queue you select here must be set to a unicast ID. The default ID for unicast queues is 1. Alternatively, you can manually enter 0 if you want the default Queue ID to be used.
- Use Queue Group: If you specified this setting, then you can only select one of the queues defined in the Queue Group Template Policy you chose in step vi.



Note 1 — If the Use Queue Group option is enabled for the global policy, then the Queue ID you select is validated against the specified Queue Group Template Policy. The Queue ID is validated against the local queues for each local policy instance.

Note 2 — You cannot delete a Queue Group Template Policy that is referenced by a queue group.

- Use Policer: If you specified this setting and disabled the Port Redirect Queue Group parameter in step v, then you can select one of the queues defined in the Queue Group Template Policy you chose in step vi. If you enabled the Port Redirect Queue Group parameter in step v, then select the required local queue here.

ix In the Hsmda Queue panel, configure the HSMDA Queue ID and Port Redirect Queue Group parameters, if applicable and required.

x Configure the parameters. You can create one entry for each of the eight forwarding class types. The parameters include:

- In Profile
- Out Profile
- In Precedence
- Out Precedence
- In DSCP
- Out DSCP
- Mark DE bit
- Force DE value

xi Click on the OK button. A dialog box appears.

xii Click on the OK button. The Forwarding Class (Create) form closes and the SAP Access Egress Policy (Create) form reappears with a list of the newly created forwarding classes displayed.

12 Perform one of the following:

a Click on the IP Match Criteria tab to configure IPv4 match criteria.

i Click on the Create button. The IP Match form opens.

ii Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Protocol
- Fragment
- HSMDA Counter Override
- Forwarding Class
- Source IP
- Src Mask
- Destination IP
- Dst Mask
- DSCP
- Source Port
- Destination Port
- Profile

The Source Port and Destination Port parameters appear only when the Protocol parameter value is TCP, UDP, or UDPTCP (*).

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The IP Match form closes and the SAP Access Egress Policy form reappears.

b Click on the IPv6 Match Criteria tab.

i Click on the Create button. The IPv6 Match form opens.

ii Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Protocol
- Forwarding Class
- HSMDA Counter Override
- Fragment
- Profile
- Source IP
- Src Mask
- Destination IP
- Dst Mask
- DSCP
- Source Port
- Destination Port

The Source Port and Destination Port parameters appear only when the Protocol parameter value is TCP or UDP.

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The IPv6 Match form closes and the SAP Access Egress Policy form reappears.

13 Click on the DSCP tab.

i Click on the Create button. The DSCP form opens.

ii Configure the parameters:

- DSCP
- HSMDA Counter Override
- Forwarding Class
- Profile

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The DSCP form closes and the SAP Access Egress Policy form reappears.

14 Click on the Precedence tab.

i Click on the Create button. The Precedence form opens.

ii Configure the parameters:

- Precedence
- HSMDA Counter Override
- Forwarding Class
- Profile

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The Precedence form closes and the SAP Access Egress Policy form reappears.

15 Click on the Dot1p tab.

i Click on the Create button. The Dot1p form opens.

ii Configure the parameters:

- Dot1p
- Forwarding Class
- Profile

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The Dot1p form closes and the SAP Access Egress Policy form reappears.

16 Click on the Apply button to save the policy. The SAP Access Egress Policy form is refreshed with additional buttons.

17 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

18 Close the SAP Access Egress Policy form. The SAP Access Egress Policies form reappears.

19 Click on the Search button to display the newly-created policy or policies in the bottom panel of the form.

Procedure 43-4 To configure a 7210 SAS or 1830 PSS port access egress policy

The 7210 SAS port access egress policy defines the SLA for service packets as they egress on the SAP. Eight queues are defined in the 7210 SAS policy. A 7210 SAS queue management policy can be associated with a queue to manage the buffer allocation for in-profile and out-of-profile packets. A 7210 SAS remarking policy with the type DOT1P or DOT1P-LSP-EXP SHARED can be associated with a 7210 SAS port access egress policy. The 7210 SAS port access egress policy can be associated with an Epipe or VPLS SAP.

1 Choose Policies→QoS→SROS QoS→Access Egress→7210 and 1830 Port Access Egress from the 5620 SAM main menu. The 7210 and 1830 Port Access Egress Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.

b Click on the Create button. The Port Access Egress Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Scope
- Egress Remark
- Remarking Type

The Remarking Type parameter is configurable when the Egress Remark parameter is set to True.

4 Perform the following to bind a remarking policy.

i Click on the Select button in the Remarking Policy panel to choose a remarking policy. The Select Remarking Policy - 7210 and 1830 Port Access Egress form opens.

ii Choose a remarking policy in the list and click on the OK button. The Select Remarking Policy - 7210 and 1830 Port Access Egress form closes and the information is displayed.

5 Click on the Queues tab. Eight default queues are displayed on the form.

i Choose a queue and click on the Properties button. The PortAccessEgressQueue, Access Egress Policy (Create) form opens with the General tab displayed.

ii Configure the parameters:

- ID
- Displayed Name
- Description

iii Click on the CIR/PIR tab.

iv Configure the parameters:

- CIR (kbps)
- PIR (kbps)
- CIR Adaptation
- PIR Adaptation

v Click on the OK button. A dialog box appears.

vi Click on the OK button.

6 Click on the Forwarding Classes tab.

i Click on the Create button. The Network Egress Forwarding Class, Port Access Egress Policy (Create) form opens.

ii Configure the parameters. You can create one entry for each of the eight forwarding class types.

- Forwarding Class
- In Profile
- Out Profile
- DSCP In Profile
- DSCP Out Profile

The DSCP In Profile and DSCP Out Profile parameters are configurable only on a Release 4.0 or later 7210 SAS-M.

iii Click on the OK button to close the Network Egress Forwarding Class, Port Access Egress Policy (Create) form. A dialog box appears.

iv Click on the OK button.

v Repeat steps 6 i to 6 iv if you need to create additional rules. You can configure up to eight rules for one policy.

7 Click on the Apply button to save the policy. The 7210 and 1830 Port Access Egress Policy (Create) form is refreshed with additional tabs.

8 Close the 7210 and 1830 Port Access Egress Policy form. The 7210 and 1830 Port Access Egress Policies form reappears.

9 Click on the Distribute button to distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

Procedure 43-5 To configure a 7210 SAS SAP access egress policy

1 Choose Policies→QoS→SROS QoS→Access Egress→7210 SAP Access Egress from the 5620 SAM main menu. The 7210 SAP Access Egress Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.

b Click on the Create button. The 7210 SAP Access Egress Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Scope
- Remarking

4 Click on the Select button in the Remarking Policy panel to choose a remarking policy. The Select Remarking Policy form opens.

5 Choose a remarking policy in the list and click on the OK button. The Select Remarking Policy form closes and the information is displayed.

6 Click on the Queues tab. Eight default queues are displayed on the form.

i Choose a queue and click on the Properties button. The QueueEntry - 7210 SAP Access Egress Policy (Create) form opens with the General tab displayed.

ii Modify the parameters, if required:

- ID
- Displayed Name
- Description
- Port Parent
- Weight
- CIR Level

iii Click on the Select button in the Queue Management Policy panel. The Select Queue Management Policy form opens.

iv Choose a queue management policy and click on the OK button. The Select Queue Management Policy form closes and the information is displayed.

v Click on the CIR/PIR tab.

vi Configure the parameters:

- CIR (%)
- PIR (%)
- CIR Adaptation
- PIR Adaptation

vii Click on the OK button. A dialog box appears.

viii Click on the OK button.

7 Click on the Apply button to save the policy. The 7210 SAP Access Egress Policy form is refreshed with additional buttons.

8 Close the 7210 SAP Access Egress Policy form. The 7210 SAP Access Egress Policies form reappears.

9 Click on the Distribute button to distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

Procedure 43-6 To configure a network policy

1 Choose Policies→QoS→SROS QoS→Network→Network from the 5620 SAM main menu. The Network Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Network Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Displayed Name
- Description
- Auto-Assign ID
- Scope
- Network Policy Type for 7705 SAR
- Default FC
- Default FC Profile
- LER Use DSCP
- Remark
- Force DSCP Remark

The Force DSCP Remark parameter is set to true.

4 Click on the Egress Forwarding Classes tab. Eight default objects based on the eight forwarding classes, as described in Table 43-1, are displayed on the form. Configure the forwarding class parameters as required.

5 Double-click on a forwarding class. The Egress Forwarding Class (Create) form opens.

6 Configure the parameters:

- Queue ID
- Policer ID
- DSCP In Profile
- LSP Exp In Profile
- Dot1p In Profile
- Mark DE bit
- DSCP Out Profile
- LSP Exp Out Profile
- Dot1p Out Profile
- Force DE value

The Queue ID parameter must be specified in the queue group template policy.

7 Click on the OK button. The Egress Forwarding Class (Create) form closes and a dialog box appears.

8 Click on the OK button. The Network Policy (Create) form reappears.

9 Click on the Ingress Forwarding Classes tab. Eight default objects based on the eight forwarding classes, as described in Table 43-1, are displayed on the form. Configure the forwarding class parameters as required.

10 Double-click on a forwarding class. The Ingress Forwarding Class (Create) form opens.

11 Configure the parameters:

- Policer ID
- Multipoint Policer ID

12 Click on the OK button. The Ingress Forwarding Class (Create) form closes and a dialog box appears.

13 Click on the OK button. The Network Policy (Create) form reappears.

14 Specify how you want to configure the mapping between the ingress or egress traffic and related queues by clicking on the appropriate tab. Mapping is optional and can be based on combinations of customer QoS marking for LSP EXP Bits, DCSP, and precedence. Table 43-6 describes the options.

Table 43-6 Network policy traffic-mapping configuration options

tab	Use
Ingress LSP EXP Bits	Maps the LSP EXP Bits of the ingress traffic to the ingress queue ID.
Ingress DCSP	Maps the DSCP of the ingress traffic to the ingress queue ID.
Ingress Dot1p	Maps the dot1p tag of the ingress traffic to the ingress queue ID.
Egress DCSP	Maps the DSCP of the egress traffic to the egress queue ID.
Egress Precedence	Maps the Precedence value of the egress traffic to the egress queue ID.

Perform the following steps for each mapping that you want to configure.

i Click on the appropriate tab.

ii Click on the Create button. A Create form opens.

iii Configure the parameters:

- LSP Exp
- DSCP
- Dot1p
- Precedence
- Forwarding Class
- Profile

The Forwarding Class and Profile parameters appear on all forms. The LSP Exp, DSCP, Dot1p, and Precedence parameters appear only on the form with the same name as the parameter.

iv Click on the OK button to close the form. The policy form reappears with the newly created object displayed.

15 Click on the Apply button to save the policy. The Network Policy form is refreshed with additional buttons.

16 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

17 Close the Network Policy form. The Network Policies form reappears.

18 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 43-7 To configure a 7210 SAS or 1830 PSS network policy

The network QoS policy consists of an ingress and egress component. The ingress component defines how dot1p, DSCP, or LSP-Exp bits are mapped to an internal forwarding class and a profile state. The ingress component also defines how the forwarding classes are mapped to meters, and defines the meters of the QoS. The egress component performs remarking, which is enabled by default but can be configured. You can associate a 7210 SAS remarking policy with a 7210 SAS network policy. You can associate a 7210 SAS remarking policy with a 7210 SAS network policy.

1 Choose Policies→QoS→SROS QoS→Network→7210 and 1830 Network from the 5620 SAM main menu. The 7210 and 1830 Network Policies form opens.

2 Perform one of the following:

- **a** Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.
- **b** Click on the Create button. The Network Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Nw Mgr ID
- Policy Id
- Auto-Assign ID
- Displayed Name
- Description
- Scope
- Type
- Default FC
- Default FC Profile
- Remarking

4 Click on the Select button in the Remarking Policy panel. The Select Remarking Policy form opens.

5 Choose a remarking policy and click on the OK button. The Select Remarking Policy form closes and the information is displayed.

6 If you are configuring a network policy for a Release 4.0 or later 7210 SAS-M or 7210 SAS-X network interface, perform the following steps.

i Configure the Meter Color Mode parameter.

ii Click on the Select button in the MPLS EXP-LSP Profile panel. The Select MPLS LSP-EXP Profile form opens.

iii Choose an MPLS LSP-EXP Profile and click on the OK button. The Select MPLS LSP-EXP Profile form closes and the information is displayed.

7 Click on the Egress Forwarding Classes tab. Eight default objects based on the eight forwarding classes, as described in Table 43-1, are displayed on the form.

8 Choose a forwarding class and click on the Properties button. The Egress Forwarding Class, Network Policy (Create) form opens.

9 Configure the parameters:

- Dot1p In Profile
- Dot1p Out Profile
- DSCP In Profile
- DSCP Out Profile

10 Click on the OK button. The Egress Forwarding Class, Network Policy (Create) form closes and a dialog box appears.

11 Click on the OK button.

12 Map the dot1p tag of the ingress traffic to the ingress queue ID, if required.

i Click on the Ingress Dot1p tab.

ii Click on the Create button. The Network Ingress Dot1p, Network Policy (Create) form opens.

iii Configure the parameters:

- Dot1p
- Forwarding Class
- Profile

iv Click on the OK button to close the form. The policy form reappears with the newly created object displayed.

v Repeat step 13 for each new rule that you need to add. You can configure up to eight rules.

13 Map the LSP EXP Bits of the ingress traffic to the ingress queue ID, if required.

i Click on the Ingress LSP EXP Bits tab.

ii Click on the Create button. The Network Ingress Lsp Exp, 7210 Network Policy (Create) form opens.

iii Configure the parameters:

- LSP Exp
- Forwarding Class
- Profile

iv Click on the OK button to close the form. The policy form reappears with the newly created object displayed.

v Repeat step 13 for each new rule that you need to add. You can configure up to eight rules.

14 Map the DSCP of the ingress traffic to the ingress queue ID, if required.

i Click on the Ingress DSCP tab.

ii Click on the Create button. The Network Ingress DSCP, Network Policy (Create) form opens.

iii Configure the parameters:

- DSCP
- Forwarding Class
- Profile

iv Click on the OK button to close the form. The policy form reappears with the newly created object displayed.

v Repeat step 13 for each new rule that you need to add. You can configure up to eight rules.

15 Click on the Ingress Meter tab and perform the following.

i Click on the Create button. The Network Ingress Meter (Create) form opens with the General tab displayed.

ii Configure the parameters:

- ID
- MultiPoint
- Mode

iii Click on the CIR/PIR tab.

iv Configure the parameters:

- CIR Adaptation
- PIR Adaptation
- CIR (kbps)
- PIR (kbps)

v Click on the Burst Size tab.

vi Configure the parameters:

- Committed Burst Size (kbps)
- Maximum Burst Size (kbps)

vii Click on the Apply button. A dialog box appears.

viii Click on the OK button.

ix Repeat steps ii to viii if you need to create additional ingress meter rules.

x Click on the Cancel button to close the Network Ingress Meter (Create) form.

16 Click on the Ingress FCMeter tab and perform the following.

i Click the Create button. The 7210 Network Ingress Forwarding Class (Create) form opens.

ii Configure the parameters:

- Forwarding Class
- Meter
- MultiCast-Meter

iii Click on the OK button. A dialog box appears.

iv Click on the OK button.

v Repeat steps ii to iv to add additional forwarding class mapping rules.

17 Click on the OK button.

18 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

Procedure 43-8 To configure a WRED slope policy

1 Choose Policies→QoS→SROS QoS→Slope→WRED Slope from the 5620 SAM main menu. The Slope Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Slope Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

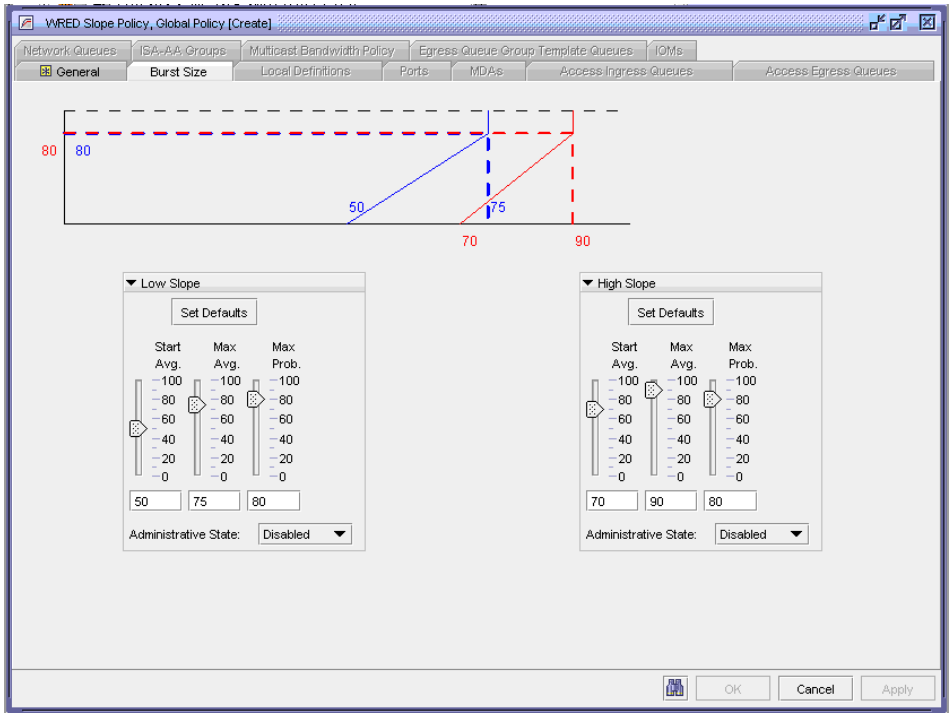
- Displayed Name
- Description
- Time Average Factor (weight)

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

When packets are queued, shared buffer average utilization is calculated using the Time Average Factor for the buffer pool. The time average factor specifies the weighting between the previous shared buffer average utilization result and the new shared buffer utilization to determine the new shared buffer average utilization.

4 Click on the Burst Size tab. The Burst Size form opens, as shown in Figure 43-4.

Figure 43-4 Slope policy form - Burst Size



Each buffer pool supports a high-priority RED slope and a low-priority RED slope. The high-priority RED slope manages access to the shared portion of the buffer pool for high-priority or in-profile packets. The low-priority RED slope manages access to the shared portion of the buffer pool for low-priority or out-of-profile packets. See "Slope policies" in this chapter for more information.

5 Configure the parameters for the Low Slope and the High Slope:

- Start Average
- Max Avg.
- Max Prob.
- Administrative State

6 Click on the Apply button to save the policy. The Slope Policy form is refreshed with additional buttons.

7 Click on the Action button and choose Distribute to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

8 Close the Slope Policy form. The Slope Policies form reappears.

9 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 43-9 To configure a 7210 SAS slope policy

The 7210 SAS supports WRED queue management. Default buffer pools are associated with each port. Each port has two associated buffer pools:

- access egress pool
- access uplink egress pool

Each pool is associated with a default slope policy that disables the low and high slopes within the pool.

1 Choose Policies→QoS→SROS QoS→Slope→7210 and 1830 Slope from the 5620 SAM main menu. The 7210 and 1830 Slope Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.

b Click on the Create button. The WRED Slope Policy, Global Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description



Note — You cannot use a colon in the Displayed Name value. The 5620 SAM uses colons as separators for the object full name.

4 If you are configuring a 7210 SAS-D 6F 4T ETR, go to step 7.

5 Click on the Burst Size tab.

6 Configure the Low Slope and High Slope parameters:

- Administrative State
- Start Threshold
- Queue1 Drop Rate
- Queue2 Drop Rate
- Queue3 Drop Rate
- Queue4 Drop Rate
- Queue5 Drop Rate
- Queue6 Drop Rate
- Queue7 Drop Rate
- Queue8 Drop Rate

7 Click on the Queue Slope tab. Eight default queues are displayed on the form.

8 Choose a queue and click on the Properties button. The QueueSlope, WRED Slope Policy, Global Policy (Create) form opens.

9 Configure the Time Average Factor parameter.

10 Configure the parameters in the High Slope panel:

- Administrative State
- Start Average
- Max Average
- Max Probability

11 Configure the parameters in the Low Slope panel:

- Administrative State
- Start Average
- Max Average
- Max Probability

12 Configure the parameters in the Non TCP Slope panel:

- Administrative State
- Start Average
- Max Average
- Max Probability

13 Click on the OK button. The QueueSlope, WRED Slope Policy Global Policy (Create) form closes and a dialog box appears.

14 Click on the OK button.

15 Repeat steps 8 to 14 for each additional queue that you need to configure. Otherwise, go to step 16.

16 Click on the Apply button to save the policy. The WRED Slope Policy, Global Policy form reappears with additional buttons.

17 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

18 Close the WRED Slope Policy, Global Policy form. The 7210 and 1830 Slope Policies form reappears.

19 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 43-10 To configure an HSMDA WRED slope policy

1 Choose Policies→QoS→SROS QoS→Slope→HSMDA WRED Slope from the 5620 SAM main menu. The HSMDA Slope Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The HSMDA Slope Policy (Create) form opens with the General tab displayed.

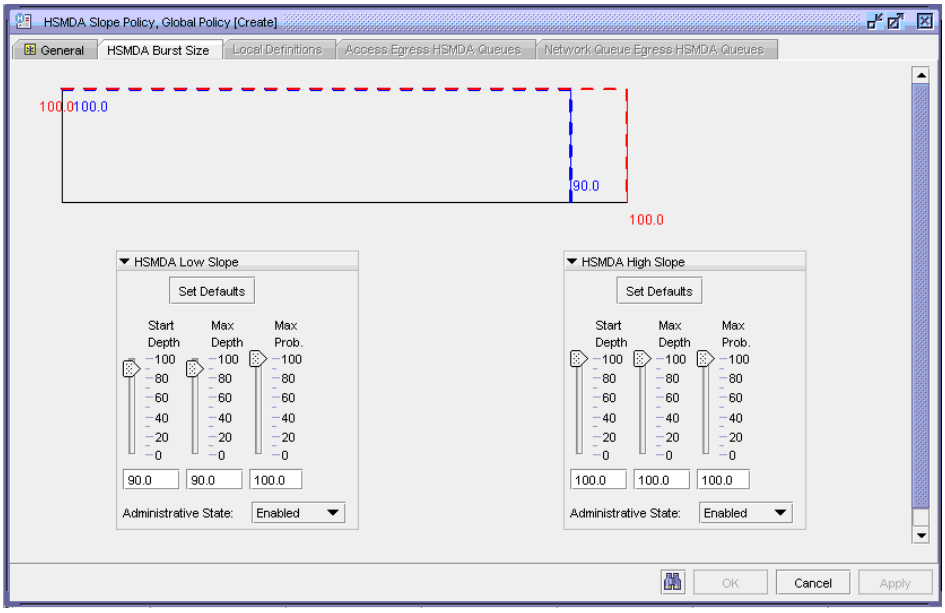
3 Configure the parameters:

- Displayed Name
- Description
- Queue MBS (bytes)

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the HSMDA Burst Size tab. The Burst Size form opens, as shown in Figure 43-5.

Figure 43-5 HSMDA Slope Policy form - Burst Size



Each buffer pool supports a high-priority RED slope and a low-priority RED slope. The high-priority RED slope manages access to the shared portion of the buffer pool for high-priority or in-profile packets. The low-priority RED slope manages access to the shared portion of the buffer pool for low-priority or out-of-profile packets. See "Slope policies" in this chapter for more information.

5 Configure the parameters for the Low Slope and the High Slope:

- Start Depth
- Max Depth
- Max Probability
- Administrative State

6 Click on the Apply button to save the policy. The HSMDA Slope Policy form is refreshed with additional buttons.

7 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

8 Close the HSMDA Slope Policy form. The HSMDA Slope Policies form reappears.

9 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 43-11 To configure a 7210 SAS queue management policy

Use a 7210 SAS queue management policy to configure slope parameters that specify a WRED profile for each queue. WRED is used to manage buffers during periods of congestion.



Note 1 — You can assign a 7210 SAS queue management policy to the queues of the following 7210 SAS policies:

- network queue policy
- access egress policy
- access ingress policy

Note 2 — Three WRED slopes per queue are supported on the 7210 SAS:

- high priority/in profile TCP
- low priority/out-of-profile TCP
- non-TCP

You can configure some 7210 SAS chassis types to use only TCP slopes (two slopes per queue). See Procedure 13-18.

Note 3 — You cannot modify a default 7210 SAS queue management policy.

1 Choose Policies→QoS→SROS QoS→Slope→7210 Queue Management from the 5620 SAM main menu. The 7210 Queue Management Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.

b Click on the Create button. The 7210 Queue Management Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Scope
- Time Average Factor



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Configure the parameters for the burst size:

- Committed Burst Size (kbps)
- Maximum Burst Size (kbps)

5 Configure the parameters for the high slope:

- Administrative State
- Start Average
- Max Average
- Max Probability

6 Configure the parameters for the low slope:

- Administrative State
- Start Average
- Max Average
- Max Probability

7 Click on the Apply button. The 7210 Queue Management Policy (Edit) form is refreshed with additional tabs.

8 Click on the following tabs to view information about a 7210 SAS queue management policy:

- Network Queues
- SAP Egress Queues
- Access Ingress Queues
- Local Definitions
- Tree
- Faults

9 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

10 Close the 7210 Queue Management Policy form. The 7210 Queue Management Policies form reappears.

11 Click on the Search button to display the newly created policies in the bottom panel of the form.

Procedure 43-12 To configure a network queue policy

You cannot use the same network queue policy on devices of different releases. For example, if the 5620 SAM manages a Release 10.0 7750 SR and a Release 11.0 7750 SR, you must create one policy for the Release 10.0 NE and one policy for the Release 11.0 NE.

1 Choose Policies→QoS→SROS QoS→Network Queue→Network Queue from the 5620 SAM main menu. The Network Queue Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Network Queue Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Configure the Packet Byte Offset parameter in the Egress HSMDA panel.

5 Click on the Select button in the WRR Policy panel to choose a WRR policy. The Select WRR Policy search form opens.

6 Select a policy in the list and click on the OK button. The Select WRR Policy form closes and the policy information is displayed on the Network Queue Policy form.

7 Click on the Apply button.

8 Click on the Egress HSMDA Queues tab. Eight default queues are displayed on the form.

9 Double-click on a queue in the list to configure a default Egress HSMDA queue. The Network Queue Egress HSMDA Queue (Edit) form opens with the General tab displayed.

10 Configure the WRR Weight parameter.



Note — The WRR Weight parameter is only displayed and configurable for Egress HSMDA Queues 1, 2, and 3.

11 Click on the Select button in the Slope Policy panel to choose a slope policy. The Select Slope Policy search form opens.

12 Select a policy in the list and click on the OK button. The Select Slope Policy form closes and the policy information is displayed on the Network Queue Egress HSMDA Queue form.

13 Click on the PIR/Burst SIze tab.

14 Configure the parameters:

- PIR (%)
- PIR Adaptation
- Maximum Burst Size (bytes)
- Burst Limit (bytes)

You must deselect the associated Default check box to configure the Maximum Burst Size (bytes) or Burst Limit (bytes) parameter.

15 Click on the OK button. The Network Queue Egress HSMDA Queue configuration form closes and the Network Queue Policy (Create) form reappears with a list of the Egress HSMDA Queues displayed.

16 Click on the Queues tab. Two default queues are displayed on the form.

17 Perform one of the following:

a To configure a default queue, double-click on a queue in the list. The Entry, Network Queue Policy (Edit) form opens with the General tab displayed.

b To create a new queue, click on the Create button. The Entry, Network Queue Policy (Create) form opens with the General tab displayed.

18 Configure the parameters:

- ID
- Displayed Name
- Description
- Pool Name
- Multipoint
- Expedite
- Port Average Overhead (%)
- Port Parent
- Level
- CIR Level
- Weight
- CIR Weight

19 Click on the Select button in the Slope Policy panel to choose a slope policy. The Select Slope Policy search form opens.

20 Select a policy in the list and click on the OK button. The Select Slope Policy form closes and the policy information is displayed on the Network Queue Policy form.

21 Click on the CIR/PIR tab.

22 Configure the parameters:

- CIR (%)
- PIR (%)
- CIR Adaptation
- PIR Adaptation

23 Click on the Burst Size tab.

24 Configure the parameters:

- High Priority Reserved (%)
- Committed Burst Size (%)
- Maximum Burst Size (%)

25 Click on the OK button. A dialog box appears.

26 Click on the OK button. The Entry, Network Queue Policy configuration form closes and the Network Queue Policy (Create) form reappears with a list of the network queues displayed.

27 Click on the Forwarding Classes tab.

28 Perform one of the following:

a To configure an existing forwarding class, click the Search button and then double-click on a forwarding class in the list. The Forwarding Class, Network Queue Policy (Edit) form opens with the General tab displayed.

b To create a new forwarding class, click on the Create button. The Forwarding Class, Network Queue Policy (Edit) form opens.

29 Configure the parameters:

- Forwarding Class
  The Forwarding Class parameter can be configured only when you are creating a forwarding class network queue policy.
- Queue ID
- Multipoint Queue ID
- Egress HSMDA Queue ID

30 Click on the OK button to close the forwarding class configuration form.

31 Click on the OK button in the dialog box that appears.

32 Click on the Apply button.

33 Click on Yes in the dialog box that appears.

34 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. The Distribute - Network Queue form opens.



Note 1 — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

Note 2 — Policies are also automatically distributed to devices when they are used by resources on the device.

Note 3 — The 5620 SAM automatically distributes an updated policy to a device when the policy is in use on the device.

i Select the devices in the Available Nodes panel to which you want to distribute the policy and click on the right arrow. The devices move to the Selected Nodes panel.

ii Click on the Distribute button. The Distribute - Network Queue form closes.

When the Policy has been successfully distributed, the selected devices will appear on the list under the Local Definitions tab.

35 Policy parameters for a specific local device can be modified by selecting the device from the Local Definitions list and clicking on Properties. The Network Queue Policy (Edit) form for the device opens. Any changes you make here will only affect the selected device.

36 Click OK to close the Network Queue Policy form. The Network Queue Policies form reappears.

37 Click on the Search button to display the newly-created policy or policies in the list panel of the form.

Procedure 43-13 To configure a 7210 SAS or 1830 PSS network queue policy

1 Choose Policies→QoS→SROS QoS→Network Queue→7210 and 1830 Network Queue from the 5620 SAM main menu. The 7210 and 1830 Network Queue Policies form opens.

2 Perform one of the following:

   a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy. The Network Queue (Edit) form opens with the General tab displayed.

   b Click on the Create button. The Network Queue (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description

4 Click on the Queues tab. Eight default queues are displayed on the form.

5 Choose a queue in the list and click on the Properties button. The NQueueEntry, Network Queue (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Displayed Name
- Description

7 Click on the Select button in the Queue Management Policy panel. The Select Queue Management Policy form opens.

8 Choose a queue management policy and click on the OK button. The Select Queue Management Policy form closes and the queue policy information is displayed.

9 Configure the parameters in the Port Parent panel:

- Port Parent
- Weight
- CIR Level

10 Click on the CIR/PIR tab.

11 Configure the parameters:

- CIR (%)
- CIR Adaptation
- CIR (%)
- PIR Adaptation

12 Click on the OK button. The NQueueEntry (Create) form closes and a dialog box appears.

13 Click on the OK button. The Network Queue (Create) form reappears with a list of the network queues displayed.

14 Click on the Forwarding Classes tab to view the eight default objects based on the eight forwarding classes, as described in Table 43-1.

15 Click on the OK button to save the settings and close the Network Queue (Create) form.

16 Click on the Distribute button to manually distribute the policy locally to devices. The Distribute - Network Queue for 7210 form opens.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

17 Click on the Apply button.

18 Close the 7210 and 1830 Network Queue Policies form.

Procedure 43-14 To modify a shared-queue policy

You cannot create shared-queue policies. Instead, you modify the existing default policy (default or policer-output-queues). Modification of shared-queue policies is supported on the 7750 SR and 7450 ESS.

Table 43-7 shows the default queue number, forwarding class, PIR, CIR, and CBS values for each shared queue.

Table 43-7 Shared queue default values

Queue #	FC	PIR (%)	CIR (%)	High priority reserved	CBS (%)	MBS (%)
1	be	100	0	10	3	25
2	l2	100	25	10	3	25
3	af	100	20	10	3	25
4	l1	100	25	10	10	50
5	h2	100	100	10	10	50
6	ef	100	100	10	10	50
7	h1	100	10	10	3	50
8	nc	100	10	10	1	50

The default behavior automatically chooses the expedited or non-expedited nature of the queue based on the forwarding classes mapped to it. As long as all forwarding classes mapped to the queue are expedited (nc, ef, h1 or h2), the queue is treated as an expedited queue by the hardware schedulers. When any non-expedited forwarding classes are mapped to the queue (be, af, l1 or l2), the queue is treated as best effort (be) by the hardware schedulers.

1 Choose Policies→QoS→SROS QoS→Shared Queue from the 5620 SAM main menu. The Shared Queue Policies form opens.

2 Choose Local or Global from the Policy scope drop-down menu. When you set it to Local, you can specify the Local Node IP Address parameter and choose a device by using the Select button and selecting a device in the list.

3 Click on the Search button. The default shared-queue policy is listed.

4 Choose the policy in the list and click on the Properties button. The Shared Queue Policy (Edit) form opens with the General tab displayed.

5 Configure the Description parameter.

6 Click on the Queues tab.

Table 43-8 list the queue IDs that are used by the 5620 SAM to identify the shared queue types.

Table 43-8 Shared queue types

Shared queue ID	Shared queue type
1 to 8	Unicast
9 to 16	Multicast
17 to 25	Broadcast
26 to 32	Unknown

There are 32 default queues are displayed on the form. Configure the queues as required. Only 16 queues are available for the policer-output-queues policy.

i Double-click on a queue in the list. The Queue configuration form opens with the General tab displayed.

ii Configure the Expedite and Pool Name parameters.



Note — Before you can configure the Pool Name parameter, you must create a Q1 pool using Procedure 43-30.

iii Click on the CIR/PIR tab.

iv Configure the parameters:

- CIR (%)
- PIR (%)

v Click on the Burst Size tab.

vi Configure the parameters:

- High Priority Reserved (%)
- Committed Burst Size (%)
- Maximum Burst Size (%)

vii Click on the OK button. The queue configuration form closes and a dialog box appears.

viii Click on the OK button.

7 Click on the Forwarding Classes tab.

Eight default objects based on the eight forwarding classes, as described in Table 43-7, are displayed on the form. You cannot associate different forwarding classes with the shared queues.

8 Click on the L2 Interfaces or L3 Interfaces tab. (Applies to default shared queue policy only.)

9 Select an interface in the list and click on the Properties button. The L2 or L3 Access Interface form opens with the General tab displayed.

10 Click on the QoS tab. (Applies to default shared queue policy only.)

11 Configure the Use Multipoint Shared Queue parameter.

12 Click on the OK button. The Shared Queue Policy form reappears.

13 Click on the Apply button to save the policy. The Shared Queue Policy (Edit) form refreshes.

To modify a local instance of the shared-queue policy, complete steps 1 to 5. Click on the Local Definitions tab. The shared-queue policies for each managed device are listed. Select a shared-queue policy in the list and click on the Properties button to modify the local instance of the policy. Complete steps 6 to 13.

Procedure 43-15 To configure a scheduler policy

1 Choose Policies→QoS→SROS QoS→Scheduler→Scheduler from the 5620 SAM main menu. The Scheduler Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Scheduler Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Frame Based Accounting

4 Click on the Apply button.

5 Click on the Schedulers tab.

The scheduler defines bandwidth control that limits each child (other schedulers and queues) that are associated with the scheduler.

6 Click on the Create button. The Entry, Scheduler Policy (Create) form opens.

7 Configure the parameters:

- Displayed Name
- Description
- Tier
- Summed CIR
- PIR (kbps)
- CIR (kbps)
- Parent Scheduler
- Level
- CIR Level
- Weight
- CIR Weight
- Port Parent
- Level
- Weight
- CIR Level
- CIR Weight

The Parent Scheduler, Level, CIR Level, Weight, and CIR Weight parameters appear only when the Tier parameter is set to 2 or 3 and the Port Parent parameter is set to false.

The Tier parameter identifies the level of hierarchy with which a group of schedulers is associated. A parent is tier 1. Children are tier 2. Grandchildren are tier 3. You can create a tier 2 child scheduler without creating a parent tier 1 scheduler, and you can create a grandchild tier 3 scheduler without creating a child tier 2 scheduler.

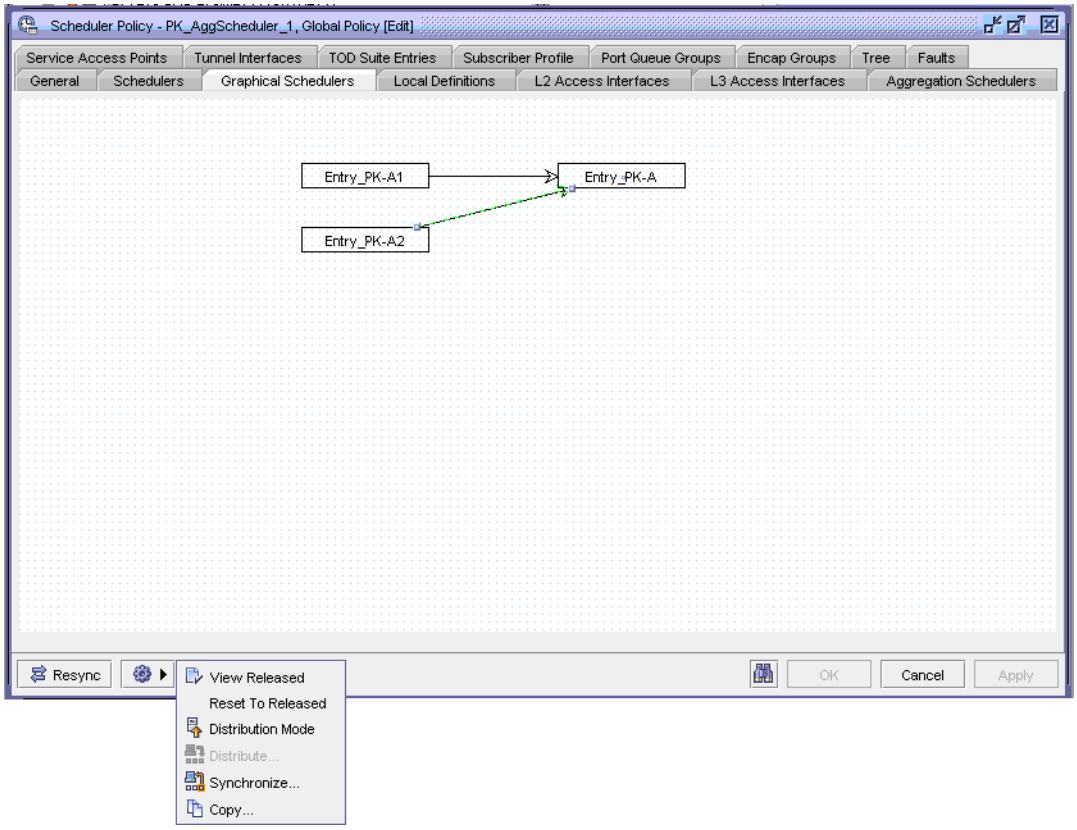
8 Click on the OK button. The Entry, Scheduler Policy (Create) form closes and a dialog box appears.

9 Click on the OK button. The newly configured scheduler is added to the list of schedulers.

10 To add additional schedulers to the policy, repeat steps 6 to 9.

11 Click on the Graphical Schedulers tab to view a graphical display of the scheduler hierarchy within the scheduler policy. An example of the graphical display is shown in Figure 43-6.

Figure 43-6 Scheduler Policy form - Graphical Schedulers



12 Click on the Apply button.

13 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

14 Close the Scheduler Policy form. The Scheduler Policies form reappears.

15 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 43-16 To configure an HSMDA scheduler policy

1 Choose Policies→QoS→SROS QoS→Scheduler→HSMDA Scheduler from the 5620 SAM main menu. The HSMDA Scheduler Policies form opens.

2 Perform one of the following:

   a Specify a filter to search for and modify an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

   b Click on the Create button. The HSMDA Scheduler Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

   - Displayed Name
   - Description
   - Maximum Rate (Mbps)



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the HSMDA Group Rates tab.

5 Configure the Rate (Mbps) parameter for group 1 and group 2.

6 Click on the HSMDA Scheduler Classes tab.

7 Configure the parameters for classes 1 to 8:

   - Group
   - Weight
   - Rate (Mbps)

   The Group parameter must be configured with the same group (Group 1 or Group 2) for up to three sequential classes for each group. For example, when you configure Class 1 as Group 2, you can configure Class 2 and Class 3 as Group 2, but not as Group 1.

   The Rate (Mbps) parameter is configurable when the Group parameter is set to None. The Weight parameter is configurable when the Group parameter is set to a value other than None.

8 Click on the Apply button.

9 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

10 Close the Scheduler Policy form. The Scheduler Policies form reappears.

11 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 43-17 To configure an HSMDA WRR policy

Perform this procedure to configure an HSMDA WRR policy.



Note — HSMDA WRR policies are supported for a Release 9.0 R3 or later 7750 SR-7 or 7750 SR-12.

1 Choose Policies→QoS→SROS QoS→Scheduler→HSMDA WRR Policy from the 5620 SAM main menu. The HSMDA WRR Policies form opens.

2 Perform one of the following:

- **a** Specify a filter to search for and modify an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.
- **b** Click on the Create button. The HSMDA WRR Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Include Queues
- Schedule Using Class
- Weight



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Apply button. The Global Policy Configuration panel appears on the form.

5 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. The Distribute HSMDA WRR Policy form opens.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

6 Select the devices you want to distribute the policy to from the list of Available Nodes and click the right-pointing arrow to move the devices into the Selected Nodes list.

7 Click the Distribute button.

When the Policy has been successfully distributed, the selected devices will appear on the list under the Local Definitions tab.

8 Policy parameters for a specific local device can be modified by selecting the device from the Local Definitions list and clicking on Properties. The HSMDA WRR Policy (Edit) form for the device opens. Any changes you make here will only affect the selected device.

9 Close the HSMDA WRR Policy form. The HSMDA WRR Policies form reappears.

The newly created policy or policies appear in the bottom panel of the form.

10 For an existing HSMDA WRR policy, you can also determine which objects currently refer to the policy by checking the following tabs, selecting an item, and clicking the Properties button:

- L2 Access Interfaces
- L3 Access Interfaces
- Network Queue Policies
- Access Egress Policies
- Subscriber Profiles

11 Close the HSMDA WRR Policies form.

Procedure 43-18 To configure a port scheduler policy

1 Choose Policies→QoS→SROS QoS→Scheduler→Port Scheduler from the 5620 SAM main menu. The Port Scheduler Policies form opens.

2 Perform one of the following:

   a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

   b Click on the Create button. The Port Scheduler (Create) form opens with the General tab displayed.

3 Configure the parameters:

   - Displayed Name
   - Description
   - Maximum Rate (kbps)



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

   The Maximum Rate (kbps) parameter is configurable when the MAX check box is deselected.

4 Click on the Group tab.

5 Click on the Create button. The Port Scheduler Group (Create) form opens.

6 Configure the parameters:

   - Displayed Name
   - PIR (kbps)
   - CIR (kbps)

   The PIR (kbps) and CIR (kbps) parameters are configurable when the associated MAX check box is deselected.

7 Click on the Apply button. A dialog box appears.

8 Click on the OK button. The Port Scheduler Group (Create) form closes and the Port Scheduler (Create) form reappears.

9 Click on the Level tab.

10 Click on the Select button in any of the Level panels to choose a port scheduler group from the list in the Select Group form. The port scheduler group must be preexisting on the port scheduler policy (see step 4).

11 Configure the parameters:

- PIR (kbps) (level 1)
- CIR (kbps) (level 1)
- Weight in group (level 1)
- PIR (kbps) (level 2)
- CIR (kbps) (level 2)
- Weight in group (level 2)
- PIR (kbps) (level 3)
- CIR (kbps) (level 3)
- Weight in group (level 3)
- PIR (kbps) (level 4)
- CIR (kbps) (level 4)
- Weight in group (level 4)
- PIR (kbps) (level 5)
- CIR (kbps) (level 5)
- Weight in group (level 5)
- PIR (kbps) (level 6)
- CIR (kbps) (level 6)
- Weight in group (level 6)
- PIR (kbps) (level 7)
- CIR (kbps) (level 7)
- Weight in group (level 7)
- PIR (kbps) (level 8)
- CIR (kbps) (level 8)
- Weight in group (level 8)
- Level
- Weight
- CIR Level
- CIR Weight



Note — Contiguous mapping of levels to a group is enforced. Priority levels cannot be added to a group unless the resulting set of priority levels is contiguous. When a level is not explicitly mapped to any group, it maps directly to the root of the port scheduler at its own priority.

The PIR (kbps) to PIR (kbps) and CIR (kbps) to CIR (kbps) parameters are each configurable when the associated MAX check box is deselected.

The Weight in group to Weight in group parameters are configurable when a port scheduler group is associated with the port scheduler policy.

12 Click on the Apply button.

13 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

14 Close the Port Scheduler Policy configuration form. The Port Scheduler Policies form reappears.

15 Close the Port Scheduler Policies form.

Procedure 43-19 To configure a 7210 SAS or 1830 PSS port scheduler policy

1 Choose Policies→QoS→SROS QoS→Scheduler→7210 and 1830 Port Scheduler from the 5620 SAM main menu. The 7210 and 1830 Port Scheduler Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.

b Click on the Create button. The Port Scheduler (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Mode



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 If you selected a value of WeightedRoundRobin or WeightedDeficitRoundRobin for the Mode parameter, go to step 5. Otherwise go to step 7.

5 Click on the Queues tab.

6 Configure the Weight parameter for queues 1 to 8.

7 Click on the Apply button.

8 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

9 Close the Port Scheduler form. The 7210 and 1830 Port Scheduler Policies form reappears.

Procedure 43-20 To configure a policer control policy

1 Choose Policies→QoS→SROS QoS→Scheduler→Policer Control from the 5620 SAM main menu. The Policer Control Policies form opens.

2 Perform one of the following steps.

a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.

b Click on the Create button. The Policer Control Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Maximum Frame Based Bandwidth
- Minimum Separation Buffer Space



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Arbiter tab.

i Click on the Create button. The Arbiter (Create) form opens.

ii Configure the parameters:

- Arbiter Name
- Description
- Tier
- Priority Level
- Weight
- Frame Based Bandwidth Rate
- Parent Arbiter

The Parent Arbiter parameter is configurable when the Tier parameter is set to 2.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The Arbiter (Create) form closes, and the Policer Control Policy form reappears.

5 (Optional step) Click on the Graphical Arbiters tab to view a graphical display of the arbiter hierarchy within the policer control policy. You can perform any of the following steps.

a Right-click on the grid and select New Arbiter from the drop-down menu. The Arbiter (Create) form opens. You can create a new arbiter, as described in step 4.

b Right-click on an arbiter object and select Edit from the drop-down menu. The Arbiter (Edit) form opens. You can change the arbiter, as described in step 4.

c Right-click on an arbiter and select Remove from the drop-down menu. The arbiter object is removed from the hierarchy.

d Click on a Tier 2 arbiter object and draw a line to a Tier 1 arbiter object. The Tier 1 arbiter becomes the parent of the Tier 2 arbiter.

6 Click on the Tree tab to view a hierarchical display of the policer control policy properties and sub components.

7 Click on the Priority Level tab to configure the MBS contribution for eight priority levels. For each level, configure the following parameters:

- Cumulative MBS Contribution
- Fixed MBS contribution

8 Click on the Apply button.

9 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

10 Close the Policer Control form. The Policer Control Policies form reappears.

Procedure 43-21 To configure a port policy

1 Choose Policies→QoS→SROS QoS→Scheduler→Port Policy from the 5620 SAM main menu. The Port Policies form opens.

2 Perform one of the following steps.

a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.

b Click on the Create button. The Port Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Select button in the Port Scheduler Policy panel. The Select Port Scheduler Policy list form opens.

5 Select a Port Scheduler Policy in the list and click on the OK button. The Select Port Scheduler Policy list form closes and the Port Policy (Create) form reappears with the port scheduler policy information displayed.

6 Click on the Apply button.

7 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

8 Close the Port Policy (Create) form. The Port Policies form reappears.

9 Close the Port Policies form.

Procedure 43-22 To configure a named buffer pool policy

To associate a Named Buffer Pool to a MDA, see Procedure 15-33.

1 Choose Policies→QoS→SROS QoS→Buffer Pool→Named Buffer Pool from the 5620 SAM main menu. The Named Buffer Pool Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Named Pool Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Name
- Description
- Default Weight
- MDA Weight
- Port Weight



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 To configure Q1 pools perform steps 3 to 10 in Procedure 43-30.

5 Click on the Apply button.

6 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

7 Close the Named Pool Policy form. The Named Buffer Pool Policies form reappears.

8 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

9 Close the Named Buffer Pool Policies form.

Procedure 43-23 To configure an ingress queue group template policy

1 Choose Policies→QoS→SROS QoS→Queue Group→Ingress Template from the 5620 SAM main menu. The Ingress Queue Group Template Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Ingress Queue Group Template Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Queues tab.

5 Perform one of the following:

a Specify a filter to search for and edit an existing queue. Use the filters to search for and open an existing queue by choosing a queue in the filtered list and clicking on the Properties button.

b Click on the Create button. The Ingress Queue, Ingress Queue Group Template Policy, Global Policy (Create) form opens with the General tab displayed.

6 Configure the parameters:

- ID
- Displayed Name
- Description
- Multipoint
- Mode
- Policed
- Expedite

7 Configure the Named Buffer Pool parameter.

i Click on the Select button beside the Named Buffer Pool parameter. The Named Buffer Pool form opens.



Note — Before you can configure the Named Buffer Pool parameter, you must create a Named Buffer Pool policy using Procedure 43-22.

ii Specify a filter to search for existing policy.

iii Select the policy and click on the OK button. The Ingress Queue, Ingress Queue Group Template Policy, Global Policy (Create) form reappears.

8 Configure the Scheduler button parameter.

i Click on the Select button beside the Scheduler button parameter. The Schedulers form opens.

ii Specify a filter to search for existing scheduler.

iii Select the scheduler and click on the OK button. The Ingress Queue, Ingress Queue Group Template Policy, Global Policy (Create) form reappears.

iv Configure the parameters in the Scheduler Association panel.

- Level
- Weight
- CIR Level
- CIR Weight

9 Configure the Advanced Configuration Policy Displayed Name parameter.

i Click on the Select button in the Advanced Configuration Policy panel to choose a policy. The Select Advanced Configuration Policy search form opens.

ii Select a policy in the list and click on the OK button. The Select Advanced Configuration Policy form closes and the chosen policy name is displayed on the Ingress Queue, Ingress Queue Group Template Policy (Create) form.

10 Configure the CIR/PIR parameters.

i Click on the CIR/PIR tab.

ii Configure the parameters:

- CIR (kbps)
- PIR (kbps)
- CIR Adaptation
- PIR Adaptation

Ensure that the CIR value is lower than the PIR value.

11 Configure the Burst Size parameters.

i Click on the Burst Size tab.

ii Configure the parameters:

- Committed Burst Size (kb)
- Maximum Burst Size (bytes)
- High Priority Reserved
- Burst Limit (kb)

The parameters are configurable when the Default check box above each is deselected.

Ensure that the Committed Burst Size (kb) value is lower than the Maximum Burst Size (bytes) value.

iii Click on the OK button. A dialog box appears.

iv Click OK.

12 Click on the Policers tab.

13 Perform one of the following:

a Specify a filter to search for and edit an existing policer. Use the filters to search for and open an existing policer by choosing a policer in the filtered list and clicking on the Properties button.

b Click on the Create button. The Ingress Policer, Ingress Queue Group Policer, Global Policy (Create) form opens with the General tab displayed.

14 Configure the parameters:

- ID
- Description
- Parent Arbiter
- Stats Mode
- Packet Byte Offset

15 Configure the Advanced Configuration Policy Displayed Name parameter.

i Click on the Select button in the Advanced Configuration Policy panel to choose a policy. The Select Advanced Configuration Policy search form opens.

ii Select a policy in the list and click on the OK button. The Select Advanced Configuration Policy form closes and the chosen policy name is displayed on the Ingress Queue, Ingress Queue Group Template Policy (Create) form.

16 Configure the CIR/PIR parameters.

i Click on the CIR/PIR tab.

ii Configure the parameters:

- Profile Capped
- CIR (kbps)
- PIR (kbps)
- CIR Adaptation
- PIR Adaptation

17 Configure the Burst Size parameters.

i Click on the Burst Size tab.

ii Configure the parameters:

- Committed Burst Size (kb)
- Maximum Burst Size (bytes)
- High Priority Reserved

The parameters are configurable when the Default check box above each is deselected.

iii Click on the OK button. A dialog box appears.

iv Click OK.

18 Close the Ingress Queue Group Template Policy form.

Procedure 43-24 To configure an egress queue group template policy

1 Choose Policies→QoS→SROS QoS→Queue Group→Egress Template from the 5620 SAM main menu. The Egress Queue Group Template Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Egress Queue Group Template Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 If you need to configure HSMDA queues go to step 5. Otherwise, go to step 17.

5 Configure the parameters:

- Packet Offset (bytes)
- Low Burst Max Class

6 Associate a WRR Policy, as required. Click the Select button in the WRR Policy panel.The Select WRR Policy form opens.

7 Select the required WRR Policy and click OK. The Select WRR Policy form closes and the Egress Queue Group Template Policy (Create) form refreshes with the WRR Policy information.

8 Click on the HSMDA Queues tab.

9 Edit the HSMDA queues as required, by selecting a queue from the list and clicking on Properties. The Egress Queue Group Template HSMDA Queue (Edit) form opens for the selected queue, and the General tab is displayed.

10 Configure the parameters:

- Displayed Name
- Description
- WRR Weight

11 Configure a Slope Policy, if required, by clicking the Select button.The Select Slope Policy form opens.

12 Select the required Slope Policy and click OK. The Select Slope Policy form closes and the Egress Queue Group Template HSMDA Queue (Edit) formrefreshes with the Slope Policy information.

13 Click on the PIR/Burst Size tab.

14 Configure the parameters:

- PIR (kbps)
- Maximum Burst Size (bytes)
- Burst Limit (bytes)
- PIR Adaptation

The sliders can be configured when the checkboxes above them are disabled.

15 Click OK. The selected HSMDA queue is revised with your configuration changes and the Egress Queue Group Template HSMDA Queue (Edit) form closes.

16 Repeat steps 5 to 15 for any other required HSMDA queues.

17 Click on the Queues tab.

18 Perform one of the following:

a Specify a filter to search for and edit an existing queue. Use the filters to search for and open an existing queue by choosing a queue in the filtered list and clicking on the Properties button.

b Click on the Create button. The Egress Queue, Egress Queue Group Template Policy, Global Policy (Create) form opens with the General tab displayed.

19 Configure the parameters:

- ID
- Displayed Name
- Description
- Port Parent
- Rate Type
- Expedite
- Level
- Weight
- CIR Level
- CIR Weight

The Level, Weight, CIR Level, and CIR Weight parameters are configurable only if the Port Parent parameter is set to True.

20 Configure the Named Buffer Pool parameter.

i Click on the Select button beside the Named Buffer Pool parameter. The Named Buffer Pool form opens.



Note — Before you can configure the Named Buffer Pool parameter, you must create a Named Buffer Pool policy using Procedure 43-22.

ii Specify a filter to search for existing policy.

iii Select the policy and click on the OK button. The Egress Queue, Egress Queue Group Template Policy, Global Policy (Create) form reappears.

21 Configure the Scheduler button parameter.

i Click on the Select button beside the Scheduler button parameter. The Schedulers form opens.



Note — The Scheduler parameter is configurable only if you set the Port Parent parameter to False.

ii Specify a filter to search for existing scheduler.

iii Select the scheduler and click on the OK button. The Egress Queue, Egress Queue Group Template Policy, Global Policy (Create) form reappears.

iv Configure the parameters in the Scheduler Association panel.

- Level
- Weight
- CIR Level
- CIR Weight

22 Configure the Advanced Configuration Policy Displayed Name parameter.

i Click on the Select button in the Advanced Configuration Policy panel to choose a policy. The Select Advanced Configuration Policy search form opens.

ii Select a policy in the list and click on the OK button. The Select Advanced Configuration Policy form closes and the chosen policy name is displayed on the Egress Queue, Egress Queue Group Template Policy (Create) form.

23 Configure the WRED Queue parameters.

i Select the Use WRED Queue parameter.

ii Click on the Select button beside the Displayed Name parameter. The Select WRED Queue Slope Policy form opens.



Note — Before you can select a WRED Queue Slope policy, you must create the policy using Procedure 43-8.

iii Specify a filter to search for existing policy.

iv Select the WRED Slope policy and click on the OK button. The Egress Queue, Egress Queue Group Template Policy, Global Policy (Create) form reappears.

24 Configure the CIR/PIR parameters.

i Click on the CIR/PIR tab.

ii Configure the parameters:

The choice of CIP and PIR parameter definitions depends on the Rate Type parameter setting on the General tab.

- CIR (kbps) - if Rate Type parameter is set to Specific
- PIR (kbps) - if Rate Type parameter is set to Specific
- CIR (Percentage) - if Rate Type parameter is set to Percentage
- PIR (Percentage) - if Rate Type parameter is set to Percentage
- CIR Adaptation
- PIR Adaptation

25 Configure the Burst Size parameters.

i Click on the Burst Size tab.

ii Configure the parameters:

- Committed Burst Size (kb)
- Maximum Burst Size (bytes)
- High Priority Reserved
- Burst Limit (kb)

The parameters are configurable when the Default check box above each is deselected.

iii Click on the OK button. The Egress Queue, Egress Queue Group Template Policy, Global Policy (Create) form closes and a dialog box appears.

iv Click on OK.

26 Click on the Forwarding Classes tab.

27 Perform one of the following:

a Specify a filter to search for and edit an existing forwarding class. Use the filters to search for and open an existing forwarding class by choosing a forwarding class in the filtered list and clicking on the Properties button.

b Click on the Create button. The Forwarding Class, Egress Queue Group Template Policy, Global Policy (Create) form opens.

28 Configure the parameters:

- Forwarding Class
- Queue ID

29 Click on the OK button. The Forwarding Class, Egress Queue Group Template Policy, Global Policy (Create) form closes and a dialog box appears.

30 Click on OK.

31 Click on the Policers tab.

32 Perform one of the following:

a Specify a filter to search for and edit an existing policer. Use the filters to search for and open an existing policer by choosing a policer in the filtered list and clicking on the Properties button.

b Click on the Create button. The Egress Policer, Egress Queue Group Policer, Global Policy (Create) form opens with the General tab displayed.

33 Configure the parameters:

- ID
- Description
- Parent Arbiter
- Stats Mode
- Packet Byte Offset

34 Configure the Advanced Configuration Policy Displayed Name parameter.

i Click on the Select button in the Advanced Configuration Policy panel to choose a policy. The Select Advanced Configuration Policy search form opens.

ii Select a policy in the list and click on the OK button. The Select Advanced Configuration Policy form closes and the chosen policy name is displayed on the Ingress Queue, Ingress Queue Group Template Policy (Create) form.

35 Configure the CIR/PIR parameters.

i Click on the CIR/PIR tab.

ii Configure the parameters:

- Profile Capped
- CIR (kbps)
- PIR (kbps)
- CIR Adaptation
- PIR Adaptation

36 Configure the Burst Size parameters.

i Click on the Burst Size tab.

ii Configure the parameters:

- Committed Burst Size (kb)
- Maximum Burst Size (bytes)
- High Priority Reserved

The parameters are configurable when the Default check box above each is deselected.

iii Click on the OK button. The Egress Policer, Egress Queue Group Policer, Global Policy (Create) form closes and a dialog box appears.

iv Click OK.

37 Close the Egress Queue Group Template Policy form.

Procedure 43-25 To configure an Advanced Configuration policy

The Advanced Configuration Policy allows for additional configurations to queues and policers in the access ingress/egress policies and the ingress/egress queue group templates. This extra configuration is subsequently applied by assigning the Advanced Configuration Policy to a queue or policer.

1 Choose Policies→QoS→SROS QoS→Scheduler→Advanced Configuration Policy from the 5620 SAM main menu. The Advanced Configuration Policy (Create) form opens with the General tab displayed.

2 Configure the parameters:

- Displayed Name
- Description



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

3 Click on the Measured Offered Rate tab.

i Configure the parameters:

- High Rate Hold Time (seconds)
- Sample Interval
- Fast Start
- Fast Stop
- Time Average Factor
- Use Time Average Factor only when offered rate is decreasing

ii Configure the parameters in the Measured Offered Rate Increase panel:

- Rate Type
- Value
- Default
- Use as minimum offered rate

  The Value parameter will either be expressed as a kbps rate or a percentage, based on your choice of Rate Type.

  The Default parameter causes the Value parameter to use whatever value is set for the entity in its own configuration form.

iii Configure the parameters in the Granularity panel:

- Rate Type
- Value
- Default

  The Value parameter will either be expressed as a kbps rate or a percentage, based on your choice of Rate Type.

  The Default parameter causes the Value parameter to use whatever value is set for the entity in its own configuration form.

iv Configure the parameters in the Max Decrement panel:

- Rate Type
- Value
- Default

  The Value parameter will either be expressed as a kbps rate or a percentage, based on your choice of Rate Type.

  The Default parameter causes the Value parameter to use whatever value is set for the entity in its own configuration form.

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The Arbiter (Create) form closes, and the Policer Control Policy form reappears.

4 Click on the Bandwidth Distribution tab.

i Configure the parameters in the Above Offered Cap panel:

- Rate Type
- Value
- Default

The Value parameter will either be expressed as a kbps rate or a percentage, based on your choice of Rate Type.

The Default parameter causes the Value parameter to use whatever value is set for the entity in its own configuration form.

ii Configure the parameters in the Granularity panel:

- Rate Type
- Value
- Default

The Value parameter will either be expressed as a kbps rate or a percentage, based on your choice of Rate Type.

The Default parameter causes the Value parameter to use whatever value is set for the entity in its own configuration form.

5 Click on the Apply button.

A number of other tabs will then become active. These allow you to view where the policy is used, once it has been assigned to the various applicable entities.

6 Click on the General tab.

7 Click on the Switch Mode button beside the Configuration Mode parameter to distribute the policy. See Procedure 42-1 for more information on how to release and distribute newly-created policies.

8 Close the Advanced Configuration Policy form.

Procedure 43-26 To configure a 7705 SAR fabric profile

1 Choose Policies→QoS→SROS QoS→7705 SAR Fabric from the 5620 SAM main menu. The marshmallowwheelFabric Profiles form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The 7705 SAR Fabric Profile (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Mode

4 Click on the Rates tab. In Aggregate mode, one rate is displayed. In Destination mode, six rates are displayed. Perform one of the following:

a For Aggregate mode, configure the Aggregate Rate parameter to set the fabric shaping rate to the daughter card slots.

b For Destination mode, configure the Rate To MDA (destRateTo1<card#> parameter for each daughter card slot to set the fabric shaping rate to each daughter card.

You can also configure the MultiPoint Rate parameter to be distributed to all of the daughter cards.

5 Click on the Apply button. The form changes to enable the other tabs.

6 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

7 Close the 7705 SAR Fabric form. The Manage 7705 SAR Fabric form is updated.

8 Click on the Search button to display the newly created profile or profiles in the bottom panel of the form.

9 Close the Manage 7705 SAR Fabric form.

Procedure 43-27 To configure a 7210 SAS remarking policy

The 7210 SAS remarking policy is used to configure the remarking behavior for the NE at the egress of the access SAPs, ports, and IP interfaces. A 7210 SAS remarking policy can be associated with the following 7210 SAS QoS policies:

- Port Access Egress Policy (the remarking policy must be DOT1P or DOT1P-LSP-EXP SHARED)
- Network Policy (the remarking policy must be LSP-EXP or DOT1P-LSP-EXP SHARED)
- Network Queue Policy (the remarking policy must be DOT1P-DSCP, DOT1P, or DSCP)

1 Choose Policies→QoS→SROS QoS→7210 Remarking from the 5620 SAM main menu. The Manage Remarking Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.

b Click on the Create button. The 7210 Remarking Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Policy Id
- Auto-Assign ID
- Displayed Name
- Description
- Type



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Apply button. The 7210 Remarking Policy (Edit) form appears with the General tab displayed.

5 Click on the Forwarding Classes tab. Eight default objects based on the eight forwarding classes, as described in Table 43-1, are displayed on the form. Configure the forwarding class parameters, as required.

6 Double-click on a forwarding class. The 7210 Remark Forwarding Class (Edit) form opens.

7 Configure the parameters:

- Dot1P-LSP-EXP-Shared In Profile
- Dot1P-LSP-EXP-Shared Out Profile

8 Click on the OK button. The 7210 Remark Forwarding Class (Edit) form closes and the 7210 Remarking Policy (Edit) form appears.

9 Click on the OK button. A dialog box appears.

10 Click on the Yes button. The 7210 Remarking Policy (Edit) form closes and the Manage Remarking Policies form appears.

11 Click on the Search button to display a list of 7210 remarking policies.

12 Choose a 7210 remarking policy and click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

Procedure 43-28 To configure a 7210 MPLS LSP-Exp Map policy

Use this procedure primarily for RSVP LSP with FRR one-to-one. For LDP LSPs, or when using FRR facility, use of a single MPLS LSP-Exp Map policy for all IP interfaces is recommended. Local LDP FC Enable needs to be set to true from CLI.

1 Choose Policies→QoS→SROS QoS→7210 MPLS LSP-Exp Map from the 5620 SAM main menu. The 7210 MPLS LSP-Exp Map Policies form opens.

2 Click on the Create button. The 7210 MPLS LSP-Exp Map Policy (Create) form opens with the general tab displayed.

3 Configure the parameters:

- Policy Id
- Auto-Assign ID
- Displayed Name
- Description



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the MPLS LSP-Exp Bits tab.

5 Select a bit from the list and click on the Properties button. The MPLS LSP-Exp Map Profile (Create) form opens.

6 Configure the Profile parameter.

7 Click on the OK button. A dialog box appears.

8 Click on the OK button. The MPLS LSP-Exp Map Profile (Create) form closes.

9 Repeat steps 5 to 8 as required.

10 Click on the OK button. The 7210 MPLS LSP-Exp Map Policy (Create) form closes.

Procedure 43-29 To configure an HSMDA pool policy

To associate an HSMDA buffer pool with an MDA, see Procedure 15-33.

1 Choose Policies→QoS→SROS QoS→Buffer Pool→HSMDA Pool from the 5620 SAM main menu. The Manage HSMDA Pool Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The HSMDA Pool Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- System Reserve (%)



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Root Pools tab.

5 Configure the Allocation Weight parameter for root pools 1 to 8.

The Allocation Weight parameter is configurable when the Default check box is deselected.

6 Click on the Class Pools tab.

7 Configure the parameters for root pools 1 to 8:

- Root Parent
- Allocation Percent

The Allocation Percent parameter is configurable when the Default check box is deselected.

8 Click on the Apply button.

9 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

10 Close the HSMDA Pool Policy form. The Manage HSMDA Pool Policies form reappears.

11 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

12 Close the Manage HSMDA Pool Policies form.

Procedure 43-30 To configure Q1 pools

You must configure a Q1 pool to before you can assign the pool to an access ingress, access egress, network queue or shared queue policy.

1 Choose Policies→QoS→SROS QoS→Buffer Pool→Named Buffer Pool from the 5620 SAM main menu. The Manage Named Buffer Pool Policies form opens.

2 Perform one of the following:

- **a** Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.
- **b** Click on the Create button. The Named Pool Policy (Create) form opens with the General tab displayed.

3 Click on Q1 Pool tab. A list of configured Q1 Pools is displayed.

4 Perform one of the following steps:

- **a** Select an existing Q1 pool. A QI Pool (Edit) form opens with the General tab displayed. Go to step 5.
- **b** Click on the Create button. A Q1 Pool (Create) form opens with the General tab displayed. Go to step 5.

5 Configure the parameters:

- Pool Name
- Description
- Network Weight
- Access Weight

6 Click on the Select button beside the Displayed Name parameter. The Select Slope Policy - Q1 Pool list form opens.

7 Select a policy in the list and click on the OK button. The Select Slope Policy - Q1 Pool list form closes and the Q1 Pool (Create) form is refreshed with the slope policy information.

8 Configure the remaining parameters:

- Reserved CBS (%)
- Default Reserved CBS
- Amber Alarm Action Max (%)
- Amber Alarm Action Step (%)
- Amber Alarm Threshold (%)
- Red Alarm Threshold (%)

9 Click on the OK button. A dialog box appears.

10 Click on the OK button. The Q1 Pool configuration form closes and the Named Pool Policy form reappears.

11 Click on the OK button. A dialog box appears.

12 Click on the OK button. The Named Pool Policy configuration form closes and the Manage Named Buffer Pool Policies form reappears.

13 Close the Manage Named Buffer Pool Policies form.

Procedure 43-31 To create an Aggregation Scheduler

You can create an Aggregation Scheduler when you have created two or more scheduler policies. See "Hierarchical schedulers" in this chapter for more information.

1 Create two or more scheduler policies, as described in Procedure 43-15.

2 Choose Manage→Service→Customers from the 5620 SAM main menu. The Manage Customers form opens.

3 Specify a filter to search for an existing customer and click on the Search button.

4 Select a customer in the list and click on the Properties button. The Customer (Edit) form opens.

5 Click on the Sites tab.

6 Select a site in the list and click on the Properties button. The Site (Edit) form opens.

7 Click on the Aggregation tab.

8 Click on the Create button. The Create Aggregation Scheduler wizard opens.

9 Select a site in the list and click on the Next button.

10 Configure the parameters:

- Scheduler Name
- Description

11 Click on the Next button. The Select Assignment Scope step is displayed.

12 Configure the Equipment Type parameter.

13 Click on the Next button. The Select Card or the Select Port step is displayed, depending on the option chosen for the Equipment Type parameter.

14 Click on the Select button to specify a card or port. The Select Card - Aggregation Scheduler form or the Select Port - Aggregation Scheduler form opens.

15 Select a card or port in the list and click on the OK button. The Select - Aggregation Scheduler form closes and the card or port information is displayed on the Select Card or Select Port form.

16 Click on the Next button. The Select Ingress and Egress Scheduler Policies step is displayed.

17 Click on the Select buttons to choose ingress and egress scheduler policies. The Select Policy - Aggregation Scheduler form opens.

18 Set the filter criteria, if required, and click on the Search button. A list of policies is displayed.

19 Select a policy in the list and click on the OK button. The Select Policy - Aggregation Scheduler form closes and the policy information is displayed in the Select Ingress and Egress Scheduler Policies form.

20 If you are creating an Aggregation Scheduler for an IOM3 port, then go to step 21. Otherwise go to step 25.

21 Click on the Next button. The Select Ingress and Egress Policer Control Policies step is displayed.

22 Click on the Select buttons to choose ingress and egress policer control policies. The Select Policer Control Policy - Aggregation Scheduler form opens.

23 Set the filter criteria, if required, and click on the Search button. A list of policies is displayed.

24 Select a policy in the list and click on the OK button. The Select Policer Control Policy - Aggregation Scheduler form closes and the policy information is displayed in the Select Ingress and Egress Policer Control Policies form.

25 Click on the Next button. The Select Time Of Day Suite Policy step is displayed.

26 Click on the Select button to choose a time of day suite. The Select Time Of Day Suite - Aggregation Scheduler form opens.

27 Select a time of day suite entry and click on the OK button. The Select Time Of Day Suite - Aggregation Scheduler form closes and the policy information is displayed in the Select Time Of Day Suite Policy form.

28 Click on the Finish button. A dialog box appears.

29 Click on the OK button. The Aggregation Scheduler is listed in the Aggregation tab of the Site (Edit) form. It will also be listed in the Aggregation Schedulers tab of the properties form for the specific object you assigned in step 15, either a card or port (including LAGs).

30 Close the Site (Edit) form. The Customer (Edit) form reappears.

31 Click on the OK button. A dialog box appears.

32 Click on the Yes button. The Customer (Edit) form closes and the Manage Customers form reappears.

33 Close the Manage Customers form.

Procedure 43-32 To configure an ANCP MSS static map

You can configure an ANCP MSS static map when you have created an ANCP policy and an Aggregation Scheduler.

1 Create an ANCP policy, as described in Procedure 54-2.

2 Create an Aggregation Scheduler, as described in Procedure 43-31.

3 Choose Manage→Service→Customers from the 5620 SAM main menu. The Manage Customers form opens.

4 Select a customer in the list and click on the Properties button. The Customer (Edit) form opens.

5 Click on the Aggregation tab.

6 Select a site in the list and click on the Properties button. The Aggregation Scheduler (Edit) form opens.

7 Click on the ANCP Static Map button.

8 Select an ANCP policy in the list and click on the Create button. The ANCP MSS Static Map (Create) form opens.

9 Configure the parameters:

- ANCP String
- Displayed Name

10 Click on the OK button. A dialog box appears.

11 Click on the OK button. The ANCP Policy is listed in the ANCP Static Map tab of the Aggregation Scheduler (Edit) form.

12 Click on the OK button to close the Aggregation Scheduler (Edit) form. The Customer (Edit) form reappears.

13 Click on the OK button. A dialog box appears.

14 Click on the Yes button.

15 Close the Manage Customers form.

Procedure 43-33 To configure an ATM QoS policy

1 Choose Policies→QoS→SROS QoS→ATM QoS from the 5620 SAM main menu. The Manage ATM QoS Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The ATM QoS Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Auto-Assign ID
- Displayed Name
- Description

4 Click on the QoS tab.

5 Configure the parameters:

- Service Category
- MIR (kbps)
- PIR (kbps)
- CDVT
- Shaping
- Policing
- Descriptor Type
- CLP Tagging

6 Click on the OK button to save the policy. The ATM QoS Policy (Create) form closes and the Manage ATM QoS Policies form reappears.

7 Click on the Search button to display the newly created policy or policies.

8 Choose a policy in the list and click on the Distribute button to manually distribute the policy locally to devices. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

9 Close the Manage ATM QoS Policies form.

Procedure 43-34 To configure an OmniSwitch QoS policy condition



Note — OmniSwitch QoS policies consist of a condition and an action. You must configure at least one condition and one action before you can create a policy.

1 Choose Policies→QoS→AOS QoS Policies from the 5620 SAM main menu. The AOS QoS Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing condition. Select a condition in the filtered list and click on the Properties button.

b Click on the Create button and choose QoS Condition. The AOS QoS Condition, Global Policy (Create) form opens with the General tab displayed.

3 Configure the Displayed Name parameter.



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Filter Properties tab. The Filter Properties form opens with the Port tab displayed.

5 Configure the parameters in the Port Match Criteria panel, if required:

- Match Source Port
- Source Slot
- Source Port
- Match Destination Port
- Destination Slot
- Destination Port

6 Click on the Layer 2 tab.

7 Configure the parameters in the MAC Match Criteria panel, if required:

- Source MAC
- Source Mask
- Destination MAC
- Destination Mask

8 Configure the Source VLAN parameter in the Source VLAN Match Criteria panel, if required.

9 Configure the Priority parameter in the 802.1p Match Criteria panel, if required.

10 Click on the Layer 3 tab.

11 Configure the parameters in the IP Match Criteria panel:

- Source IP
- Source Mask
- Source Net Mask
- Destination IP
- Destination Mask
- Destination Net Mask
- VRF Status
- VRF Name

12 Configure the parameters in the DSCP Match Criteria panel, if required:

- Differentiated Services Code Point
- Mask

13 Configure the parameters in the ToS Match Criteria panel, if required:

- ToS Precedence
- Mask

14 Configure the parameters in the ICMP Match Criteria panel, if required:

- ICMP Code
- ICMP Type

15 Click on the Layer 4 tab.

16 Configure the IP Protocol parameter.

The following parameters are not displayed when the IP Protocol parameter is set to HOPOPT.

17 Configure the parameters in the IP Port Match Criteria panel, if required:

- Match Source IP Port Range
- Source IP Port (Start)
- Source IP Port (End)
- Match Destination IP Port Range
- Destination IP Port (Start)
- Destination IP Port (End)

18 Click on the OK button. The AOS QoS Condition, Global Policy (Create) form closes.

19 To create more QoS policy conditions, repeat steps 2b to 18.

20 Close the AOS QoS Policies form.

Procedure 43-35 To configure an OmniSwitch QoS policy action



Note — OmniSwitch QoS policies consist of a condition and an action. You must configure at least one condition and one action before you can create a policy.

1 Choose Policies→QoS→AOS QoS Policies from the 5620 SAM main menu. The AOS QoS Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing action. Select an action in the filtered list and click on the Properties button.

b Click on the Create button and choose QoS Action. The AOS QoS Action, Global Policy (Create) form opens with the General tab displayed.



Note 1 — You cannot use DSCP and ToS parameters in the same action.

Note 2 — You cannot use Maximum Bandwidth (Kbps) and Information Rate and Burst Size parameters in the same action.

3 Configure the Displayed Name parameter.



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Configure the Action parameter in the Disposition panel.

5 Configure the parameters in the Priority and Bandwidth panel:

- Priority
- Maximum Bandwidth (Kbps)
- Share Resources

6 Configure the Priority parameter in the 802.1p panel.

7 Configure the Differentiated Services Code Point parameter in the DSCP panel.

8 Configure the Type of Service parameter in the ToS panel.

9 Configure the parameters in the Redirect panel, if required.

- Slot
- Port
- LAG Number

10 Configure the parameters in the Information Rate and Burst Size panel, if required.

- CIR (bps)
- CBS (bytes)
- PIR (bps)
- PBS (bytes)

11 Click on the OK button. The AOS QoS Action, Global Policy (Create) form closes.

12 To create more actions, repeat steps 2b to 11.

13 Close the AOS QoS Policies form.

Procedure 43-36 To create an OmniSwitch QoS policy



Note — OmniSwitch QoS policies consist of a condition and an action. You must configure at least one condition and one action before you can create a policy.

1 Choose Policies→QoS→AOS QoS Policies from the 5620 SAM main menu. The AOS QoS Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing policy. Select a policy in the filtered list and click on the Properties button.

b Click on the Create button and choose QoS Policy. The AOS QoS Policy, Global Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Policy Status
- Precedence



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Select button in the Action panel to choose an action for the policy. The Select Action - QoS Policy form opens with a list of available actions displayed.

5 Select an action and click the OK button. The Select Action - QoS Policy form closes and the AOS QoS Policy, Global Policy (Create) form refreshes.

6 Click on the Select button in the Condition panel to choose a condition for the policy. The Select Action - QoS Policy form opens with a list of available conditions displayed.

7 Select a condition and click the OK button. The Select Condition - QoS Policy form closes and the AOS QoS Policy, Global Policy (Create) form refreshes.

8 To create more policies, repeat steps 2b to 9.

9 Click on the OK button. The AOS QoS Policy, Global Policy (Create) form closes and the AoS QoS Policies form reappears.

10 Click on the Search button to display the newly created policy or policies.

11 Select a policy and click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

12 Close the AOS QoS Policies form.

Procedure 43-37 To create an OmniSwitch QoS list

This procedure is used to configure a QoS list, which is a collection of QoS polices. This QOS list includes support of egress policy configurations to perform last minute operations on the data traffic before it egresses through the port.

See Procedures 43-34, 43-35, and 43-36 to create AOS QoS policy actions, policy conditions, and policies.

1 Choose Policies→QoS→AOS QoS Policies from the 5620 SAM main menu. The AOS QoS Policies form opens.

2 Click on the Create button and choose QoS List. The AOS QoS List, Global Policy (Create) form opens with the General tab displayed.

3 Configure the following parameters:

- Displayed Name
- List Type
- Policy Status



Note — Do not use a colon to create the displayed name because the 5620 SAM uses colons as separators for the object full name.

4 To add an AOS QoS policy to the QoS list, click on the List Policies tab.

5 Click on the Create button. The AOS QoS Policy List, AOS QoS List, Global Policy (Create) form opens.

6 Click on the Select button. The Select Policy Name - QoS Policy List- AOS QoS List, Global Policy form opens.

7 Select a policy entry. Click on the OK button. The Select Policy Name - QoS Policy List- AOS QoS List, Global Policy form closes.

8 The Select Policy Name - QoS Policy List- AOS QoS List, Global Policy form reappears, with the policy name selected in Step 7 displayed in the Displayed Name field.

9 Click on the Properties button. The AOS QoS Policy -<policy name>, Global Policy (Edit) form opens.

10 If required, configure the Precedence parameter.

11 Close the AOS QoS Policy -<policy name>, Global Policy (Edit) form

12 The AOS QoS Policy List, AOS QoS List, Global Policy (Create) form reappears. Click on the OK button. A dialog box appears.

13 Click on the OK button.

14 Close the AOS QoS Policy, Global Policy (Create) form.

Procedure 43-38 To create or configure a MC MLPPP ingress QoS profile

1 Choose Policies→QoS→SROS QoS→MLPPP→Ingress QoS Profile from the 5620 SAM main menu. The Manage MLPPP Ingress QoS Profile form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing profile. Use the filters to search for and open an existing profile by choosing a profile in the filtered list and clicking on the Properties button.



Note — You can edit the properties of the default ingress MC profile, but you cannot delete the profile.

b Click on the Create button. The MLPPP Ingress QoS Profile (Create) form opens with the General tab displayed.

3 Configure the following parameters:

- Auto-Assign ID
- Profile ID
- Description

4 Click on the Apply button. The MLPPP Ingress QoS Profile (Edit) form opens with the General tab displayed.

5 Click on the Classes tab.

6 Select a class in the list and click on the Properties button. The MlpppIngressQosProfileClass (Edit) form opens.

7 Configure the Reassembly Timeout (msec) parameter.

8 Click on the OK button to save the values and close the form.

9 Repeat steps 6 to 8 for each class that you need to configure.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The MLPPP Ingress QoS Profile (Edit) form closes.

12 Click on the Search button to display any newly created policy or policies in the bottom panel of the form.

13 Close the Manage MLPPP Ingress QoS Profile form.

Procedure 43-39 To create or configure a MC MLPPP egress QoS profile

1 Choose Policies→QoS→SROS QoS→MLPPP→Egress QoS Profile from the 5620 SAM main menu. The Manage MLPPP Egress QoS Profile form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing profile. Use the filters to search for and open an existing profile by choosing a profile in the filtered list and clicking on the Properties button.



Note — You can edit the properties of the default egress MC profiles, but you cannot delete them.

b Click on the Create button. The MLPPP Egress QoS Profile (Create) form opens with the General tab displayed.

3 Configure the following parameters:

- Auto-Assign ID
- Profile ID
- Description

4 Click on the Apply button. The MLPPP Egress QoS Profile (Edit) form opens with the General tab displayed.

5 Click on the Classes tab.

6 Select a class in the list and click on the Properties button. The MlpppEgressQosProfileClass (Edit) form opens.

7 Configure the following parameters:

- MIR (%)
- Weight (%)
- Maximum Queue Size (msec)

8 Click on the OK button to save the changes and close the form.

9 Repeat steps 6 to 8 for each class that you need to configure.

10 Click on the Forwarding Classes tab.

11 Select a forwarding class in the list and click on the Properties button. The MlpppEgressQosProfileForwardingClass (Edit) form opens.

12 Configure the MLPPP Class parameter.

13 Click on the OK button to save the values and close the form.

14 Repeat steps 11 to 13 for each forwarding class that you need to configure.

15 Click on the OK button. A dialog box appears.

16 Click on the Yes button. The MLPPP Ingress QoS Profile (Edit) form closes.

17 Click on the Search button to display any newly created policies in the bottom panel of the form.

18 Close the Manage MLPPP Egress QoS Profile form.

Procedure 43-40 To create or configure an MCFR ingress QoS profile

1 Choose Policies→QoS→SROS QoS→MCFR→Ingress QoS Profile from the 5620 SAM main menu. The Manage MCFR Ingress QoS Profile form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing profile. Use the filters to search for and open an existing profile by choosing a profile in the filtered list and clicking on the Properties button.



Note — You can edit the properties of the default ingress MC profile, but you cannot delete the profile.

b Click on the Create button. The MCFR Ingress QoS Profile (Create) form opens with the General tab displayed.

3 Configure the following parameters:

- Auto-Assign ID
- Profile ID
- Description

4 Click on the Apply button. The MCFR Ingress QoS Profile (Edit) form opens with the General tab displayed.

5 Click on the Classes tab.

6 Select a class in the list and click on the Properties button. The MCFR Ingress QoS Profile Class (Edit) form opens.

7 Configure the Reassembly Timeout (msec) parameter.

8 Click on the OK button to save the values and close the form.

9 Repeat steps 6 to 8 for each class that you need to configure.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The MCFR Ingress QoS Profile (Edit) form closes.

12 Click on the Search button to display any newly created policies in the bottom panel of the form.

13 Close the Manage MCFR Ingress QoS Profile form.

Procedure 43-41 To create or configure an MCFR egress QoS profile

1 Choose Policies→QoS→SROS QoS→MCFR→Egress QoS Profile from the 5620 SAM main menu. The Manage MCFR Egress QoS Profile form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing profile. Use the filters to search for and open an existing profile by choosing a profile in the filtered list and clicking on the Properties button.



Note — You can edit the properties of the default egress MC profile, but you cannot delete the profile.

b Click on the Create button. The MCFR Egress QoS Profile (Create) form opens with the General tab displayed.

3 Configure the following parameters:

- Auto-Assign ID
- Profile ID
- Description

4 Click on the Apply button. The MCFR Egress QoS Profile (Edit) form opens with the General tab displayed.

5 Click on the Classes tab.

6 Select a class in the list and click on the Properties button. The MCFR Egress QoS Profile Class (Edit) form opens.

7 Configure the following parameters:

- MIR (%)
- Weight (%)
- Maximum Queue Size (msec)

8 Click on the OK button to save the changes and close the form.

9 Repeat steps 6 to 8 for each class that you need to configure.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The MCFR Egress QoS Profile (Edit) form closes.

12 Click on the Search button to display any newly created policies in the bottom panel of the form.

13 Close the Manage MCFR Egress QoS Profile form.

Procedure 43-42 To configure QoS policy overrides on an L2 or L3 access interface

Perform this procedure to override settings associated with an access ingress, access egress, or scheduler policy on an L2 or L3 access interface configured for a service.

See the following procedures for information about overriding access ingress, access egress, or scheduler policies that are associated with residential subscribers:

- Procedure 54-17 for the overrides associated with SLA profiles
- Procedure 54-18 for the overrides associated with subscriber profiles

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Expand Access Interface (Service Management) in the object type drop-down list and choose one of the following:

- L2 Access Interface (Service Management)
- L3 Access Interface (Service Management)

3 Configure a filter, if required, and click on the Search button. A list of L2 or L3 access interfaces is displayed.

4 Choose an interface in the list and click on the Properties button. The L2 Access Interface (Edit) form or L3 Access Interface (Edit) form opens.

5 Perform one of the following:

a Create an override for an access ingress or access egress policy queue. Go to step 6.

b Create an override for an access egress policy HSMDA queue. Go to step 15.

c Create an override for an ingress or egress policy policer. Go to step 25.

d Create an override for an ingress or egress policer control policy. Go to step 34.

e Create an override for an ingress or egress scheduler policy. Go to step 46.

6 Click on the Override Policy Items tab and perform one of the following:

a Click on the Access Ingress Queues tab.

b Click on the Access Egress Queues tab.

7 Click on the Create button.The Access Ingress Queue Override form or the Access Egress Queue Override form opens with the General tab displayed.

8 Click on the Select button in the Ingress QoS Policy Queue panel. The Select QoS Policy Queue form opens.

9 Choose a policy queue and click on the OK button. The queue override form reappears with the configured values for the selected policy queue displayed.

10 Click on the Override tab.

11 Configure the parameters, as required:

- PIR
- CIR
- Maximum Burst Size
- Committed Burst Size
- High Priority Reserved
- PIR Adaptation
- CIR Adaptation
- Queue Weight
- Queue CIR Weight
- Port Average Overhead

Overrides for the PIR and CIR are configured in kbps if the Rate Type for the queue was originally set to kbps. The PIR and CIR overrides are configured as a percentage (%) if the Rate Type for the queue was originally set to Percent Port Limit or Percent Local Limit.

The Port Average Overhead parameter is only configurable for access egress queues.

To override parameters, you must select the associated check box. De-select the associated Default or MAX check box to enter a specific value, or to select a drop-down option.

12 Click on the OK button. The queue override form closes and a dialog box appears.

13 Click on the OK button. The L2 Access Interface (Edit) form or L3 Access Interface (Edit) form is displayed.

14 Go to step 55.

15 Click on the Override Policy Items tab.

16 Click on the Access Egress HSMDA Queues tab.

17 Click on the Create button.

The Access Egress HSMDA Queue Override form opens with the General tab displayed.

18 Choose the queue that you want to override.

i Click on the Select button. The Select Access Egress Policy Queue form opens.

ii Choose the queue.

iii Click on the OK button. The Access Egress HSMDA Queue Override form reappears with the configured values for the queue.

19 Click on the Override tab.

20 Configure the parameters:

- PIR (kbps)
- Maximum Burst Size (bytes)
- WRR Weight

If you select the Override check box for a parameter, the original parameter value is displayed.

To specific another override value for the PIR (kbps) parameter, you must first deselect the associated MAX check box. To specific another override value for the Maximum Burst Size (bytes) parameter you must first deselect the associated Default check box.

You can only specify an override value for WRR Weight for queues 1, 2, or 3.

21 Choose the HSMDA Slope policy that you want to override.

i Click on the Select button. The Select HSMDA Slope Policy form opens.

ii Select the policy.

iii Click on the OK button. The queue override form reappears with the selected HSMDA Slope policy name displayed.

22 Click on the OK button. A dialog box appears.

23 Click on the OK button. The queue override form closes and the L2 Access Interface form or L3 Access Interface form reappears.

24 Go to step 55.

25 Click on the Override Policy Items tab. Perform one of the following actions.

a Click on the Ingress Policer tab.

b Click on the Egress Policer tab.

26 Click on the Create button. The policer override form opens.

27 Click on the Select button. The select policy policer form opens.

28 Select a policy policer and click on the OK button. The select policy policer form closes and the policer override form refreshes with the configured values for the policy policer.



Note — Policy policers must be applied to the L2 Access Interface or the L3 Access Interface in order to be selected.

29 Click on the Override tab.

30 Select the Override check box for any of the following parameters, and then configure the parameters:

- Override PIR
- Override CIR
- Override Maximum Burst Size
- Override Committed Burst Size
- Override Packet Offset
- Stats Mode

Overrides for the PIR and CIR are configured in kbps if the Rate Type for the policer was originally set to kbps. The PIR and CIR overrides are configured as a percentage if the Rate Type for the policer was originally set to Percent Local Limit.

To override any of these parameters, you must select the required check box. Deselect the associated Default or MAX check box to enter a specific value, or to select a drop-down parameter option.

31 Click on the OK button. A dialog box appears.

32 Click on the OK button. The policer override form closes and the L2 Access Interface form or L3 Access Interface form reappears.

33 Go to step 55.

34 Click on the Override tab. Perform one of the following actions.

a Click on the Ingress Policer Control tab.

b Click on the Egress Policer Control tab.



Note — Policer control policies must be applied to the L2 Access Interface or the L3 Access Interface in order to enable the policer control tabs.

35 Click on the Create button. The policer override form opens.

36 Select the Override check box for any of the following parameters, and then configure the parameters:

- Maximum Frame Based Bandwidth
- Minimum Separation Buffer Space

37 Click on the Level Override Policy Items tab.

38 Select a Level Override from the list and click on the Properties button. The policy policer level override form opens with the General tab displayed.

39 Click on the Override tab.

40 Select the Override check box, and then configure the Maximum Cumulative Buffer Space parameter.

41 Click on the OK button. A dialog box appears.

42 Click on the OK button. The policy policer level override form closes and the policer override form reappears.

43 Click on the OK button. A dialog box appears.

44 Click on the OK button. The policer override form closes and the L2 Access Interface form or L3 Access Interface form reappears.

45 Go to step 55.

46 Click on the Schedulers tab.

47 Choose the scheduler policy that you want to override.

i Click on the Select button to define the Ingress Scheduler and Egress Scheduler policy that you want to modify.

ii Choose the scheduler policy.

iii Click on the Apply button. A dialog box appears.

iv Click on the Yes button. The L2 Access Interface form or L3 Access Interface form reappears.

48 Click on the Override Policy Items tab.

49 Perform one of the following actions.

a Modify the Ingress Scheduler parameters.

i Click on the Ingress Schedulers tab.

ii Click on the Create button.

The Ingress policy scheduler override form opens with the General tab displayed.

b Modify the Egress Scheduler parameters.

i Click on the Egress Schedulers tab.

ii Click on the Create button.

The Egress policy scheduler override form opens with the General tab displayed.

50 Choose the scheduler policy that you want to override.

i Click on the Select button. The Select Scheduler Policy Entry form opens.

ii Choose the policy entry.

iii Click on the OK button. The policy scheduler override form reappears with the configured values for the scheduler policy.

51 Click on the Override tab.

52 Configure the parameters:

- Override Summed CIR
- Summed CIR
- Override PIR
- PIR (kbps)
- Override CIR
- CIR (kbps)

53 Click on the OK button. A dialog box appears.

54 Click on the OK button. The scheduler entry override form closes and the L2 Access Interface form or L3 Access Interface form reappears.

55 Click on the OK button to close the L2 Access Interface form or L3 Access Interface form.

Procedure 43-43 To configure QoS policy overrides on access ingress policy meters for the 7210 SAS

Perform this procedure to override the meter settings of an access ingress policy for an L2 access interface on a 7210 SAS, Release 6.0 R1 or later.

Policy overrides on 7210 SAS NEs are not supported for the following:

- Uplink SAPs
- SAPs on mirror services
- QoS policies whose scope is set to exclusive
- SAPs with time of day suites attached

1 Open the properties form for the L2 access interface for which you need to configure an override.

i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

ii Choose Site (Service Management) from the object drop down menu.

iii Configure the filter criteria, if required, and click on the Search button. A list of sites is displayed.

iv Choose a 7210 SAS site in the list and click on the Properties button. The properties form for the site opens.

v Expand the site equipment tree as required, and click on an L2 access interface. The properties form for the L2 access interface opens, with the General tab displayed.

2 Click on the Override Policy Items tab.

3 Click on the Access Ingress Meters tab.

4 Click on the Create button. The Access Ingress Meter Override (Create) form opens with the General tab displayed.

5 Click on the Select button in the Ingress QoS Policy Meter panel. The Select Ingress QoS Policy Meter form opens.

6 Choose a policy meter and click on the OK button. The Access Ingress Meter Override (Create) form reappears with the values for the selected Ingress QoS Policy Meter displayed.

7 Click on the Override tab.

8 Configure the parameters, as required:

- PIR (kbps)
- CIR (kbps)
- Maximum Burst Size (kbps)
- Committed Burst Size (kbps)
- PIR Adaptation
- CIR Adaptation
- Mode

To override parameters, you must select the associated check box. Deselect the associated Default or MAX check box to enter a specific value, or to select a drop-down menu option.

9 Click on the OK button. The Access Ingress Meter Override (Create) form closes and a dialog box appears.

10 Click on the OK button.

11 Click on the OK or Apply button on the properties form to commit the changes. A dialog box appears.

12 Click on the Yes button to confirm the changes.

Procedure 43-44 To configure QoS policy overrides on access ingress queues for a 7210 SAS-X

Perform this procedure to override the queue settings of an access ingress policy for an L2 access interface on a 7210 SAS-X, Release 6.0 R1 or later.

Policy overrides on 7210 SAS NEs are not supported for the following:

- Uplink SAPs
- SAPs on mirror services

- QoS policies whose scope is set to exclusive
- SAPs with time of day suites attached

1 Open the properties form for the L2 access interface for which you need to configure an override.

   i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

   ii Choose Site (Service Management) from the object drop down menu.

   iii Configure the filter criteria, if required, and click on the Search button. A list of sites is displayed.

   iv Choose the required 7210 SAS-X site in the list and click on the Properties button. The properties form for the site opens.

   v Expand the site equipment tree as required, and click on an L2 access interface. The properties form for the L2 access interface opens, with the General tab displayed.

2 Click on the Override Policy Items tab.

3 Click on the Access Ingress Queues tab.

4 Click on the Create button. The Access Ingress Queue Override (Create) form opens, with the General tab displayed.

5 Click on the Select button in the Ingress QoS Policy Queue panel. The Select Ingress QoS Policy Queue - SAS Access Policy Queue Override form opens.

6 Choose a queue in the list and click on the OK button. The Access Ingress Queue Override (Create) form reappears, with the information for the selected queue displayed on the General tab.



Note — You can configure an override only on a queue that is mapped to a forwarding class.

7 Click on the Override tab and configure the parameters as required:

- PIR (kbps)
- CIR (kbps)
- PIR Adaptation
- CIR Adaptation
- PIR Weight
- CIR Level

To override parameters, you must select the associated check box. Deselect the associated Default or MAX check box to enter a specific value, or to select a drop-down menu option.

8 To override the queue management policy, select the check box for Displayed Name, click on the Clear button, then click on the Select button. The Select Queue Management Policy - SAS Access Policy Queue Override form opens.

9 Choose a queue management policy from the list and click on the OK button. The Access Ingress Queue Override (Create) form reappears with the Displayed Name for the selected queue management policy displayed.



Note — The selected queue management policy must be distributed to the NE that contains the SAP for which you are performing the policy override. Click on the Properties button to view the properties form for the queue management policy. You can use this properties form to distribute the policy to the NE, if required. See "Policy distribution" in chapter 42.

10 Click on the OK button. The Access Ingress Queue Override (Create) form closes and a dialog box appears.

11 Click on the OK button.

12 Click on the OK or Apply button on the properties form to commit the changes. A dialog box appears.

13 Click on the Yes button to confirm the changes.

44 — Filter policies

44.1 Filter policies overview *44-2*

44.2 Filter policies procedures *44-4*

44.1 Filter policies overview

Filter policies specify a forward, drop, or HTTP redirect action for packets based on information specified as the match criteria. You can create up to 2000 IP and 2000 MAC filter policies per managed NE. You can create up to 131 071 entries in a filter policy.

Filter entry matching criteria are either general or specific, but all conditions must be met for the packet to be considered a match and the specified entry action performed. The process stops when the first complete match is found and the action defined in the entry is executed.

When an interface or circuit is not configured with a filter policy, all traffic is allowed. By default, there are no filters associated with services or interfaces.

The 5620 SAM supports the creation and management of the following filter policies:

- ACL MAC filter policies—applied to access interfaces and service tunnels
- ACL IP filter policies—applied to network and access IP interfaces, and service tunnels
- ACL IPv6 filter policies—applied to access interfaces and service tunnels
- ACL VLAN filter policies—applied to access interfaces
- DHCP filter policies—applied to IES and VPRN group interfaces
- LI MAC filter policies—applied to 5620 SAM LI user accounts
- Block Reservation filter policies—applied to 5620 SAM LI user accounts



Note — The 7705 SAR does not support IPv6 and MAC ACL filters.

The 7705 SAR has the following configuration limits for ACL IP filter entries:

- For non-extended range filter entries, the match criteria cannot be defined to match more than 256 packets.
- For extended range filter entries, there is no limit on the number of packet matches for the defined criteria; however, the total number of unique match criteria in use across all extended range filter entries within the same ACL IP filter cannot exceed eight.

Shared filter entries

RADIUS attributes can be used to enhance a locally configured IPv4 or IPv6 filter list with dynamic entries that can be shared between multiple subscriber hosts.

The ACL IP filter policy and ACP IPv6 filter policy include a High Watermark and Low Watermark configuration which specifies alarm thresholds for dynamically-inserted filter table counts.

SAP and service tunnel forwarding

ACL IP and ACL MAC filters contain options for delivering packets to specific destination SAPs and service tunnels based on the match criteria. Because the forwarding action is specified separately from device configuration, the packet destination name must be entered directly in text form (for example, 1/1/2:500) and validated by the 5620 SAM. Consider the following before you create a SAP or service tunnel forwarding filter:

- Although you can configure them on other service types, you should only create these filters on a VPLS. On other service types, packets are dropped.
- You can apply these filters on an ingress, but not an egress, SAP or service tunnel.
- The destination SAP or service tunnel must be on the same service as the device on which the filter is applied.
- The encapsulation type of the destination SAP and the associated port must be the same. Supported encapsulations are Ethernet Null, dot1q, QinQ, BCP, bridged Ethernet, FR, and ATM.

Embedded filter policies

The 5620 SAM supports the use of embedded filter policies in ACL filters. An embedded filter policy defines a common filter policy which can be reused by many other filter policies. The embedded policy is deployed by including (embedding) it in other exclusive or template filter policies. An exclusive or template filter policy may embed multiple embedded filter policies and conversely, a single embedded filter policy may be embedded in many exclusive or template filter policies.

When an exclusive or template filter policy that embeds one or more embedded filter policies is created, absolute values for all filter policy entries for both embedded and embedding filters are preserved. In the case of a conflict between entries (for instance, the same policy entry index), a higher priority filter entry is activated. The embedding filter has the highest priority, allowing its filter entries to always overwrite any embedded filter entries. This allows for customization of the common embedded filter policy rules within the embedding filter.

Any edits made to an embedded policy are automatically applied to all embedding filter policies that use the embedded filter policy.

The system ensures that system and hardware resources exist when a new embedded filter policy is created, changed or embedded by another filter policy, and either fails the configuration attempt or does not embed the embedded filter (depending on what resources are exhausted). An embedded filter is never embedded partially into another filter. If a change occurs to an already embedded filter fails due to a lack of hardware resources, the embedded filter will be removed from the embedding filter.

Web portal redirect

ACL IP and ACL MAC filters contain options for redirecting hosts to a URL address. The 7950 XRS, 7710 SR, 7750 SR-7, and 7750 SR-12 open a new connection to the specified web portal. The host can use the web portal to create or modify a service profile. The web portal updates the ACL policy directly, or through another system such as the 5750 SSC, to remove the redirection policy.



Note — The 7750 SR-1 does not support web portal redirect.

44.2 Filter policies procedures

The following procedures describe how to configure filter policies.

Procedure 44-1 To configure an ACL MAC filter policy



Note — ACL MAC filters are not supported for the 7705 SAR.

1 Choose Policies→Filter→ACL MAC Filter from the 5620 SAM main menu. The ACL MAC Filter Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Select a policy in the filtered list and click on the Properties button. The ACL MAC Filter (Edit) form opens with the General tab displayed.

b Click on the Create button. The ACL MAC Filter (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Filter ID
- Auto-Assign ID
- Displayed Name
- NE Filter Name
- Description
- Scope
- Default Action
- MAC Filter Type

The Default Action parameter specifies the action to be applied to packets when no action is specified in the MAC filter entries or when the packets do not match the specified criteria.

4 Configure the filter entries. Perform the following:

i Click on the Filter Entries tab.

ii Click on the Create button. The Entry, ACL MAC Filter (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Auto-Assign ID
- Entry ID
- Displayed Name
- Description
- Entry type
- Log ID
- Administrative State

iv Assign a time range to the ACL MAC filter entry by clicking on the Select button beside the Name parameter. The Select Time Range - MacFilterEntry list form opens.

v Select a time range entry and click on the OK button. The Select Time Range - MacFilterEntry list form closes and the Entry, ACL MAC Filter (Create) form refreshes with the time range information.



Note — ACL filters that include ACL filter entries to which you have assigned a time range cannot be assigned to a time of day suite policy.

Time ranges with which you have associated a ACL filter within a time of day suite policy cannot be assigned to ACL filter entries of that ACL filter.

vi Click on the Filter Properties tab.

vii Configure the Action parameter:

If you specify forward (SAP), the Forwarding Destination tab is displayed. Perform the following:

- Click on the Forwarding Destination tab.
- Configure the parameters:
  - Port Name
  - Outer Encap Value
  - Inner Encap Value

If you specify forward (SDP), the Forwarding Destination tab is displayed. Perform the following:

- Click on the Forwarding Destination tab.
- Configure the parameters:
  - Path ID
  - VC ID

If you specify HTTP redirect, the Web Redirect tab is displayed. Perform the following:

- Click on the Web Redirect tab.
- Configure the Redirect URL parameter.

viii Click on the Filter Properties tab.

ix Configure the parameters:

- Frame Type
- Source MAC
- Src Mask
- Destination MAC
- Dst Mask
- Dot1p
- Dot1p Mask
- Low ISID
- High ISID
- Inner Tag Value
- Inner Tag VID Mask
- Outer Tag Value
- Outer Tag VID Mask
- DSAP
- DSAP Mask
- SSAP
- SSAP Mask
- SNAP OUI
- SNAP PID
- Ether Type

The Source MAC, Src Mask, Destination MAC, Dst Mask, Dot1p, Dot1p Mask, Low ISID and High ISID parameter pairs are configurable when the check box for each pair is selected.

The Low ISID and High ISID parameters are only configurable when the MAC Filter Type parameter is set to ISID.

The Inner Tag Value, Inner Tag VID Mask, Outer Tag Value, and Outer Tag VID Mask parameters are only configurable when the MAC Filter Type parameter is set to VID.

The DSAP, DSAP Mask, SSAP, and SSAP Mask parameters are configurable when the Frame Type parameter value is set to e802dot2LLC and the MAC Filter Type parameter is set to Normal.

The SNAP OUI and SNAP PID parameters are configurable when the Frame Type parameter value is e802dot2SNAP and the MAC Filter Type parameter is set to Normal.

The Ether Type parameter is configurable only when the Frame Type parameter value is set to Ethernet II and the MAC Filter Type parameter is set to Normal.

x Click on the OK button. The Entry, ACL MAC Filter (Create) form closes and a dialog box appears.

xi Click on the OK button. The ACL MAC Filter (Create) form reappears with the newly created filter entry displayed.

5 By default, all IDs for filter entries are set to 0. Perform one of the following steps:

a Continue configuring the filter. Go to step 7.

b Reorder new or existing filter entries, using the New Entry ID parameter.

i Click on the Refresh button to find an existing filter entry. The list of filter entries is displayed.

ii Select a filter entry in the list.

iii Click on the Renumber ID button. The renumber entry ID form opens and displays the current filter ID.

iv Specify the New Entry ID parameter. The range is 1 to 65535.

v Click on the OK button. The renumber entry ID form closes and the list of filter entries is refreshed, based on the new ID number assigned to the filter.

6 To add an additional filter entry, repeat steps 4 and 5.

7 Click on the OK button to save the policy. The ACL MAC Filter (Create) form closes and the ACL MAC Filter Policies form reappears.

8 Click on the Search button to display the newly created policy or policies.

9 Select a policy in the list and click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.



Caution 1 — Distributing a global ACL MAC filter policy with no filter entries (either because none have been created or all existing ones have been deleted) can cause a service outage. You should ensure that the policy has at least one filter entry, or you must be certain that distributing an empty policy is what you really intend to do. A global policy will be distributed to all of the policy's local definitions.

If you attempt the manual distribution of an empty policy, two warning confirmations will be issued. The first warning is issued when you change the policy's Configuration Mode on the General tab from Draft to Released. You can either choose to proceed by clicking Yes, or abort the Configuration Mode change by clicking No.

The second warning is issued if you changed the policy's Configuration Mode to Released and then try to proceed with the actual distribution in the Distribute form. You can either choose to proceed by clicking Yes, or abort the distribution by clicking No.

Caution 2 — If you attempt to release an ACL MAC filter policy that has been initialized from an NE, you will also receive a warning confirmation, since the global policy may be partially updated from the local policy. The Discovery State indicator on the General tab displays this Initialized condition, and the Origin indicator identifies the NE. You should manually synchronize with a specific local policy before changing the Configuration Mode from Draft to Released.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

10 Close the ACL MAC Filter Policies form.

Procedure 44-2 To configure an ACL IP filter policy

1 Choose Policies→Filter→ACL IP Filter from the 5620 SAM main menu. The ACL IP Filter Policies form opens.

2 Perform one of the following:

a Specify a filter to search for an existing policy. Select a policy in the filtered list and click on the Properties button. The ACL IP Filter (Edit) form opens with the General tab displayed.

b Click on the Create button. The ACL IP Filter (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Filter ID
- Auto-Assign ID
- Displayed Name
- Scope
- NE Filter Name
- Description
- Default Action
- Use IPv6 Resource

4 Click on the Insertion Blocks tab.

5 If required, enable the check box in the Host Shared Filter Configuration panel and configure the parameters:

- High Watermark
- Low Watermark

6 Configure the parameters:

- Credit Control Start Entry
- Credit Control Count
- RADIUS Start Entry
- RADIUS Count
- Host Shared Start Entry
- Host Shared Count
- High WaterMark (%)
- Low WaterMark (%)

7 Perform the following steps to configure a filter entry.

i Click on the Filter Entries tab.

ii Click on the Create button. The Entry, ACL IP Filter (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Entry ID
- Auto-Assign ID
- Displayed Name
- Description
- Log ID
- Administrative State

iv To assign a time range to the filter entry, click on the Select button in the Time Range panel. The Select Time Range - Ipv6FilterEntry list form opens. Otherwise, go to step 7 vi.

v Select a time range entry and click on the OK button. The Select Time Range - Ipv6FilterEntry list form closes and the Entry, ACL IPv6 Filter (Create) form refreshes with the time range information.



Note — ACL filters that include ACL filter entries to which you have assigned a time range cannot be assigned to a time of day suite policy.

Time ranges with which you have associated a ACL filter within a time of day suite policy cannot be assigned to ACL filter entries of that ACL filter.

vi Click on the Filter Properties tab.

vii Configure the Action parameter:

- Click on the Next Hop Routing tab.
- Configure the parameters:
  - Forward NH
  - Is Indirect
  - Forward NH Interface
  - Remark DSCP
  - Remark DSCP Mask
  - Remark Dot1p

If you specify forward (SAP), the Forwarding Destination tab appears. Perform the following:

- Click on the Forwarding Destination tab.
- Configure the parameters:
  - Port Name
  - Outer Encap Value
  - Inner Encap Value

If you specify forward (SDP), the Forwarding Destination tab is configurable. Perform the following:

- Click on the Forwarding Destination tab.
- Configure the parameters:
  - Path ID
  - VC ID

viii On the Filter Properties tab, configure the parameters:

- Protocol
- DSCP
- Source IP
- Src Mask
- Source IP Prefix
- Destination IP
- Dst Mask
- Destination IP Prefix
- Fragment
- Source Port
- Dest Port
- IP Option
- IP Opt Mask
- Option Present
- Multiple Option
- ICMP Code
- ICMP Type
- TCP Syn
- TCP Ack
- Source Route Option

The Source Port and Dest Port parameters are configurable only when the Protocol parameter value is TCP, UDP, or UDPTCP (*).

The TCP Syn and TCP Ack parameters are configurable when the Protocol parameter value is TCP.

The ICMP Code and ICMP Type parameters are configurable when the Protocol parameter value is ICMP.

ix Click on the Cflowd tab.

x Configure the parameters:

- Cflowd Sample
- Cflowd If Sample

xi Click on the OK button. The Entry, ACL IP Filter (Create) form closes and a dialog box appears.

xii Click on the OK button. The ACL IP Filter (Create) form reappears with the newly created filter entry displayed.

8 To create an additional filter entry, repeat step 7.

9 To define the order in which the policy tries to match filter entries with packets, perform the following steps for each filter entry.

i Select a filter entry in the list.

ii Click on the Renumber ID button. The Renumber Entry ID form opens.

iii Configure the New Entry ID parameter.

iv Click on the OK button. A dialog box appears.

v Click Yes to apply the change. The Renumber Entry ID form closes, and the Entry ID column displays the new identifier assigned to the entry.

10 Click on the OK button to save the policy. The ACL IP Filter form closes and the ACL IP Filter Policies form reappears.

11 Click on the Search button to display the newly created policy or policies.

12 Select the newly created policy in the list and click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.



Caution 1 — Distributing a global ACL IP filter policy with no filter entries (either because none have been created or all existing ones have been deleted) can cause a service outage. You should ensure that the policy has at least one filter entry, or you must be certain that distributing an empty policy is what you really intend to do. A global policy will be distributed to all of the policy's local definitions.

If you attempt the manual distribution of an empty policy, two warning confirmations will be issued. The first warning is issued when you change the policy's Configuration Mode on the General tab from Draft to Released. You can either choose to proceed by clicking Yes, or abort the Configuration Mode change by clicking No.

The second warning is issued if you changed the policy's Configuration Mode to Released and then try to proceed with the actual distribution in the Distribute form. You can either choose to proceed by clicking Yes, or abort the distribution by clicking No.

Caution 2 — If you attempt to release an ACL IP filter policy that has been initialized from an NE, you will also receive a warning confirmation, since the global policy may be partially updated from the local policy. The Discovery State indicator on the General tab displays this Initialized condition, and the Origin indicator identifies the NE. You should manually synchronize with a specific local policy before changing the Configuration Mode from Draft to Released.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

13 Select the distributed policy in the list and click on the Properties button. The ACL IP Filter Global Policy (Edit) form opens.

14 Click on the Local Definitions tab.

15 Select a local definition from the list and click on the Properties button. The ACL IP Filter Local Policy (Edit) form opens.

16 Click on the Insertion Blocks tab.

17 If required, enable the check box in the Host Shared Filter Configuration panel and configure the parameters:

- High Watermark
- Low Watermark

18 Configure the parameters:

- Credit Control Start Entry
- Credit Control Count
- RADIUS Start Entry
- RADIUS Count
- Host Shared Start Entry
- Host Shared Count
- High WaterMark (%)
- Low WaterMark (%)



Note — The Group Entries Inserted panel displays the number of entries inserted on this filter range.

19 Configure the Application and Location parameters in the Group Insertion Sorting panel.

20 Click on the Sort Group Insertions button. A dialog box appears.

21 Click on the OK button.

22 Perform the following steps to view filter entry data.

i Click on the Filter Entries tab.

ii Click on the Credit Control Entries tab or the RADIUS Entries tab.

iii Click on the Search button.

iv Select an entry from the list and click on the Properties button. A form opens.

v Close the form after viewing the filter entry data.

23 Close the ACL IP Filter Entry Local Policy (Edit) form.

24 Close the ACL IP Filter Entry Global Policy (Edit) form.

25 Close the ACL IP Filter Policies form.

Procedure 44-3 To configure an ACL IPv6 filter policy



Note — The 7705 SAR does not support ACL IPv6 filters.

1 Choose Policies→Filter→ACL IPv6 Filter from the 5620 SAM main menu. The ACL IPv6 Filter Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Select a policy in the filtered list and click on the Properties button. The ACL IPv6 Filter (Edit) form opens with the General tab displayed.

b Click on the Create button. The ACL IPv6 Filter (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Filter ID
- Auto-Assign ID
- Displayed Name
- NE Filter Name
- Description
- Scope
- Default Action
- IPv6 Address Format



Note — You can only configure the IPv6 Address Format parameter when the system resource profile settings are appropriate. See Procedure 13-20.

4 Click on the Insertion Blocks tab.

5 If required, enable the check box in the Host Shared Filter Configuration panel and configure the parameters:

- High Watermark
- Low Watermark

6 Configure the parameters:



Note — These parameters are not required for 7210 SAS nodes.

- Credit Control Start Entry
- Credit Control Count
- RADIUS Start Entry
- RADIUS Count
- Host Shared Start Entry
- Host Shared Count
- High WaterMark (%)
- Low WaterMark (%)

7 Perform the following steps to configure a filter entry.

i Click on the Filter Entries tab.

ii Click on the Create button. The Entry, ACL IPv6 Filter, Global Policy (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Entry ID
- Auto-Assign ID
- Displayed Name
- Description
- Log ID
- Administrative State

iv To assign a time range to the ACL IPv6 filter entry, click on the Select button in the Time Range panel. The Select Time Range - Ipv6FilterEntry list form opens. Otherwise, go to step 7 vi.

v Select a time range entry and click on the OK button. The Select Time Range - Ipv6FilterEntry list form closes and the Entry, ACL IPv6 Filter (Create) form refreshes with the time range information.



Note — ACL filters that include ACL filter entries to which you have assigned a time range cannot be assigned to a time of day suite policy.

Time ranges with which you have associated a ACL filter within a time of day suite policy cannot be assigned to ACL filter entries of that ACL filter.

vi Click on the Filter Properties tab.

vii Configure the Action parameter:

If you specify Forward, the Next Hop Routing tab appears. Perform the following:

- Click on the Next Hop Routing tab.
- Configure the parameters:
  - Forward NH
  - Is Indirect

viii On the Filter Properties tab, configure the parameters:

- Protocol
- DSCP
- Source IP
- Src Mask
- Source IP Prefix
- Destination IP
- Dst Mask
- Destination IP Prefix
- Fragment
- Authentication Header
- Encapsulating Security Payload Header
- Source Port
- Dest Port
- ICMP Code
- ICMP Type
- TCP Syn
- TCP Ack

The Source Port and Dest Port parameters are configurable when the Protocol parameter value is TCP or UDP.

The TCP Syn and TCP Ack parameters are configurable when the Protocol parameter value is TCP.

The ICMP Code and ICMP Type parameters are configurable when the Protocol parameter value is IPv6_ICMP.

ix Click on the OK button. The Entry, ACL IPv6 Filter (Create) form closes and a dialog box appears.

x Click on the OK button. The ACL IPv6 Filter (Create) form displays the new filter entry.

8 To create an additional filter entry, repeat steps 7.

9 To define the order in which the policy tries to match filter entries with packets, perform the following steps for each filter entry.

i Select a filter entry in the list.

ii Click on the Renumber ID button. The Renumber Entry ID form opens.

iii Configure the New Entry ID parameter.

iv Click on the OK button. The Renumber Entry ID form closes, and the Entry ID column displays the new identifier assigned to the entry.

10 Click on the OK button. The ACL IPv6 Filter (Create) form closes, and the ACL IPv6 Filter Policies form reappears.

11 Click on the Search button to display the newly created policy.

12 Select the policy in the list and click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.



Caution 1 — Distributing a global ACL IPv6 filter policy with no filter entries (either because none have been created or all existing ones have been deleted) can cause a service outage. You should ensure that the policy has at least one filter entry, or you must be certain that distributing an empty policy is what you really intend to do. A global policy will be distributed to all of the policy's local definitions.

If you attempt the manual distribution of an empty policy, two warning confirmations will be issued. The first warning is issued when you change the policy's Configuration Mode on the General tab from Draft to Released. You can either choose to proceed by clicking Yes, or abort the Configuration Mode change by clicking No.

The second warning is issued if you changed the policy's Configuration Mode to Released and then try to proceed with the actual distribution in the Distribute form. You can either choose to proceed by clicking Yes, or abort the distribution by clicking No.

Caution 2 — If you attempt to release an ACL IPv6 filter policy that has been initialized from an NE, you will also receive a warning confirmation, since the global policy may be partially updated from the local policy. The Discovery State indicator on the General tab displays this Initialized condition, and the Origin indicator identifies the NE. You should manually synchronize with a specific local policy before changing the Configuration Mode from Draft to Released.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

13 Select the distributed policy in the list and click on the Properties button. The ACL IPv6 Filter Global Policy (Edit) form opens.

14 Click on the Local Definitions tab.

15 Select a local definition from the list and click on the Properties button. The ACL IPv6 Filter Local Policy (Edit) form opens.

16 Click on the Insertion Blocks tab.

17 If required, enable the check box in the Host Shared Filter Configuration panel and configure the parameters:

- High Watermark
- Low Watermark

18 Configure the parameters:

- Credit Control Start Entry
- Credit Control Count
- RADIUS Start Entry
- RADIUS Count
- Host Shared Start Entry
- Host Shared Count
- High WaterMark (%)
- Low WaterMark (%)



Note — The Group Entries Inserted panel displays the number of entries inserted on this filter range.

19 Configure the Application and Location parameters in the Group Insertion Sorting panel.

20 Click on the Sort Group Insertions button. A dialog box appears.

21 Click on the OK button.

22 Perform the following steps to view filter entry data:

i Click on the Filter Entries tab.

ii Click on the Credit Control Entries tab or the RADIUS Entries tab.

iii Click on the Search button.

iv Choose an entry from the list and click on the Properties button. A form opens.



Note — Some parameters may not be supported on the local definition of the policy, depending on the device. See "Policy distribution" and "Policy audits" in chapter 42.

v Close the form after viewing the filter entry data.

23 Close the ACL IPv6 Filter Entry Local Policy (Edit) form.

24 Close the ACL IPv6 Filter Entry Global Policy (Edit) form.

25 Close the ACL IPv6 Filter Policies form.

Procedure 44-4 To configure an ACL VLAN filter policy

An ACL VLAN filter policy can be configured on a 2-port ring MDA on the 7705 SAR-8 or 7705 SAR-18, Release 6.0 R1 or later. Only the first two ports in network mode on the 2-port ring MDA can be configured with an ACL VLAN filter policy.

1 Choose Policies→Filter→ACL VLAN Filter from the 5620 SAM main menu. The ACL VLAN Filter Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Select a policy in the filtered list and click on the Properties button. The ACL VLAN Filter, Global Policy (Edit) form opens with the General tab displayed.

b Click on the Create button. The ACL VLAN Filter (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Filter ID
- Auto-Assign ID
- Filter Name
- NE Filter Name
- Description
- Default Action

4 Perform the following steps to configure a filter entry.

i Click on the Filter Entries tab.

ii Click on the Create button. The Entry, ACL VLAN Filter, Global Policy (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Entry ID
- Auto-Assign ID
- Displayed Name
- Description
- Administrative State

iv Click on the Filter Properties tab.

v Configure the parameters:

- Action
- Operation
- Vlan 1
- Vlan 2

vi Click on the OK button. The Entry, ACL VLAN Filter, Global Policy (Create) form closes and a dialog box appears.

vii Click on the OK button. The ACL VLAN Filter (Create) form displays the new filter entry.

viii Repeat steps ii to vii to create additional filters.

ix Click on the Apply button. A dialog box appears.

x Click on the Yes button. The ACL VLAN Filter (Create) form closes.

5 To distribute a newly created policy, see Procedure 42-1.

6 To associate the ACL VLAN Filter Policy with an Ethernet port on a 2-port ring MDA on a 7705 SAR-8 or 7705 SAR-18, see Procedure 16-1.

Procedure 44-5 To configure an IP Prefix List

1 Choose Policies→Filter→IP Prefix List from the 5620 SAM main menu. The Filter - IP Prefix Lists form opens.

2 Click the Create button. The Filter - IP Prefix List (Create) form opens with the General tab displayed.

3 Configure the parameters:

- IP Prefix List Type
- IP Prefix List Name
- Description

4 Click on the IP Prefix List Members tab.

5 Click the Create button.

The IP Prefix List Member (Create) form opens.

6 Configure the parameters:

- Prefix
- Mask

7 Click OK. A dialog box appears.

8 Click OK. The newly-defined member appears on the list.

9 Repeat steps 5 to 8 to create additional members, as required.

10 Click on the Apply Path Members tab.

11 Click the Create button.

The Apply Path Member (Create) form opens.

12 Configure the parameters:

- Source
- Index
- Group
- Neighbor

13 Click OK. A dialog box appears.

14 Click OK. The new entry appears on the list.

15 Repeat steps 11 to 14 to create additional members, as required.

16 Click on the OK button to save the policy. A confirmation dialog box appears.

17 Click Yes. The Filter - IP Prefix List (Create) form closes and the new IP Prefix List appears on the list.

18 To distribute the policy, select the newly created policy in the list and click on the Properties button. The Filter - IP Prefix List (Edit) form opens with the General tab displayed.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

19 Perform the required steps in Procedure 42-1 to distribute the policy.

20 To associate a newly-created IPv4 IP Prefix List to an ACL IP Filter policy, refer to Procedure 44-2. For ACL IPv6 filters, refer to Procedure 44-3. In either of those procedures, you can specify an IP Prefix List by configuring the Source IP Prefix and/or the Destination IP Prefix parameters for a filter entry.

21 To associate a newly-created IPv4 or IPv6 IP Prefix List to a CPM Filter policy, refer to the *5620 SAM System Administrator Guide*.

22 Close the Filter - IP Prefix List (Edit) form.

23 Close the Filter - IP Prefix Lists form.

Procedure 44-6 To configure a filter Port List

1 Choose Policies→Filter→Port List from the 5620 SAM main menu. The Filter - Port Lists form opens.

2 Click the Create button. The Filter - Port List (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Port List Name
- Description

4 Click on the Port List Members tab.

5 Click the Create button.

The Port List Member (Create) form opens.

6 Configure the Port parameter.

This can either be a specific port number or a range of port numbers. For a specific port number, use the EQUAL operator from the drop down menu. For a range of port numbers, use the RANGE operator.

7 Click OK. A dialog box appears.

8 Click OK. The newly-defined member appears on the list.

9 Repeat steps 5 to 8 to create additional members, as required.

10 Click on the OK button to save the policy. A confirmation dialog box appears.

11 Click Yes. The Filter - Port List (Create) form closes and the new Port List appears on the Filter - Port List form.

12 To distribute the policy, select the newly-created policy in the list and click on the Properties button. The Filter -Port List (Edit) form opens with the General tab displayed.



Note — When the policy is in Draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Release - Filter Port List window, where you can select which NEs to distribute the policy to. See Chapter 42 for more information.

13 Perform the required steps in Procedure 42-1 to release and distribute the policy.

14 To associate a newly-created Port List to a CPM Filter policy, refer to the *5620 SAM System Administrator Guide*.

15 Close the Filter - Port List (Edit) form.

16 Close the Filter - Port Lists form.

Procedure 44-7 To configure a DHCP filter policy

1 Choose Policies→Filter→DHCP Filter from the 5620 SAM main menu. The DHCP Filter Policies list form opens.

2 Perform one of the following:

a Specify a filter to search for and modify a policy. Choose a policy and click on the Properties button. The DHCP Filter (Edit) form opens with the General tab displayed.

b Click on the Create button. The DHCP Filter (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Filter ID
- Auto-Assign ID
- Displayed Name
- Description

4 Configure a filter entry.

i Click on the Filter Entries tab.

ii Click on the Create button. The Entry, DHCP Filter (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Entry ID
- Auto-Assign ID
- Displayed Name

iv Click on the Filter Properties tab.

v Configure the parameters:

- Action
- DHCP Option
- Match Condition

The Match Condition parameter is configurable only when a DHCP Option has been selected.

vi If the Match Condition parameter is set to Match String, configure the parameters:

- Match String Type
- Match Type
- Match String

vii Click on the OK button. The Entry, DHCP Filter (Create) form closes and a dialog box appears.

viii Click on the OK button. The DHCP Filter form reappears with the newly created filter entry displayed.

5 Repeat step 4 to create up to four filter entries for a DHCP policy filter.

6 Click on the OK button to save the policy. The DHCP Filter form closes and the DHCP Filter Policies list form reappears with the new DHCP filter policy listed.

7 Choose the newly created policy and click on the Distribute button to distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

8 Choose the distributed policy in the list and click on the Properties button. The DHCP Filter Global Policy (Edit) form opens.

9 Click on the Local Definitions tab.

10 Choose a local definition from the list and click on the Properties button. The DHCP Filter Local Policy (Edit) form opens with the General tab displayed.

11 Click on the Group Interfaces tab to view IES or VPRN group interfaces that are bound to the DHCP filter policy. See Procedures 70-12 and 71-60 for more information on binding IES and VPRN group interfaces to DHCP filter policies.

12 Perform the following steps to view filter entry data.

- **i** Select an entry from the list and click on the Properties button. A form opens.
- **ii** Close the form after viewing the filter entry data.

13 Close the DHCP Filter Entry Local Policy (Edit) form.

14 Close the DHCP Filter Entry Global Policy (Edit) form.

15 Close the DHCP Filter Policies list form.

Procedure 44-8 To configure an LI MAC filter policy

Note 1 — You are required to be a 5620 SAM user with LI privileges to access the LI MAC filter policy. See chapter 28 for more information.

Note 2 — You require at least one ACL MAC filter policy to complete this procedure. See Procedure 44-1 for more information.

Note 3 — You require at least one Block Reservation policy to complete this procedure. See Procedure 44-9 for more information.

1 Choose Policies→Filter→LI Policies→LI MAC Filter from the 5620 SAM main menu. The LI MAC Filter Policies form opens.

2 Perform one of the following:

a Specify a filter to search for an existing policy. Select a policy in the filtered list and click on the Properties button. The LI MAC Filter, Global Policy (Edit) form opens with the General tab displayed.

b Click on the Create button. The LI MAC Filter, Global Policy (Create) form opens.

3 Configure the parameters:

- Displayed Name
- Description

4 Click on the LI MAC Filter Entries tab.

5 Click on the Create button. The LI MAC Filter Entry, LI MAC Filter, Global Policy (Create) form opens.

6 Configure the parameters:

- Entry ID
- Frame Type
- Source MAC
- Src Mask
- Destination MAC
- Dst Mask

7 Click on the OK button. The LI MAC Filter, Global Policy (Create) form reappears.

8 Click on the MAC Filter Association tab.

9 Click on the Create button. The LI MAC Filter Association, LI MAC Filter form opens.

10 Associate an ACL MAC filter to the LI MAC filter policy by clicking on the Select button beside the Displayed Name parameter. The Select MAC Filter - LI Mac Filter Filter Association, Global Policy form opens with a list of ACL MAC filter policies.

11 Choose an ACL MAC filter policy and click on the OK button. The LI MAC Filter, Global Policy (Create) form reappears.

12 Click Apply button to apply the changes.

13 To associate more ACL filters, repeat steps 4 to 11.

14 Click on the Search button to display the newly created LI MAC Filter policy or policies.

15 Select a policy in the list and click on the Distribute button to manually distribute the policy locally to devices. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

16 Close the LI MAC Filter Policies form.

Procedure 44-9 To configure a Block Reservation policy

Note 1 — You are required to be a 5620 SAM user with LI privileges to access the Block Reservation policy. See chapter 28 for more information.

Note 2 — You require at least one ACL MAC filter policy to complete this procedure. See Procedure 44-1 for more information.

1 Choose Policies→Filter→LI Policies→Block Reservation from the 5620 SAM main menu. The Block Reservation Policies form opens.

2 Perform one of the following:

a Specify a filter to search for an existing policy. Select a policy in the filtered list and click on the Properties button. The Block Reservation, Global Policy (Edit) form opens with the General tab displayed.

b Click on the Create button. The Block Reservation, Global Policy (Create) form opens.

3 Configure the parameters:

- Displayed Name
- Description
- Block Start
- Block Size

4 Click on the MAC Filter Association tab.

5 Click on the Create button. The LI Block Reservation Association, Block Reservation, Global Policy (Create) form opens.

6 Associate an ACL MAC filter to the Block Reservation policy by clicking on the Select button beside the Displayed Name parameter. The Select MAC Filter - LI Block Reservation - Block Reservation Global Policy form opens with a list of ACL MAC filter policies.

7 Choose an ACL MAC filter policy and click on the OK button. The LI MAC Filter, Global Policy (Create) form reappears.

8 Click the OK button to apply the changes and close the form. The Block Reservation Policies form reappears.

9 To create additional Block Reservation policies, repeat steps 1 to 8.

10 Click on the Search button to display the newly created Block Reservation policy or policies.

11 Select a policy in the list and click on the Distribute button to manually distribute the policy locally to devices. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

12 Close the Block Reservation Policies form.

Procedure 44-10 To configure a Filter Log

You can configure a Filter Log for use with IP, IPv6, and MAC filter entries.

1 Choose Policies→Log Configuration. The Manage Log Configuration Policies form opens.

2 Perform one of the following:

a Specify Filter Log (Node Log Policy) and click on the Search button to search for an existing Filter Log. Select a policy in the filtered list and click on the Properties button. The Filter Log, Global Policy (Edit) form opens with the General tab displayed.

b Click on the Create button and select Filter Log from the menu. The Filter Log, Global Policy (Create) form opens.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Log Description
- Log Destination
- SysLog Id (configured using the Select button)
- Maximum Number of Entries
- Log Stop On Full
- Log Enabled
- Log Summary Enabled
- Log Summary Criterion

The SysLog Id, Log Summary Enabled, and Log Summary Criterion parameters are only configurable when you choose the SysLog option as the Log Destination.

The Maximum Number of Entries parameter is only configurable when you choose the Memory option as the Log Destination.

4 Click on the Apply button. The Policy Configuration block is displayed.

5 Click on the Switch Mode button to distribute the policy to the required NEs. A confirmation message is displayed. Click Yes. The Release - Filter Log form opens.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

6 Select the required NEs from the list of Available Objects on the left and move them to the Selected Objects list on the right using the right-pointing arrow.

7 Click on the Distribute button. The Status field in the Selected Objects list provides the status of the distribution.

8 Close the Release - Filter Log form.

9 Close the Filter Log form.

10 Associate the Filter log to a filter entry for any of the following filter types by configuring the Log ID parameter in the associated procedure:

- ACL MAC Filter. Refer to Procedure 44-1.
- ACL IP Filter. Refer to Procedure 44-2.
- ACL IPv6 Filter. Refer to Procedure 44-3.

  The Log ID you specify in any of these procedures will refer to the Filter Log's ID parameter configured in step 3.

Procedure 44-11 To configure a Sys Log

You can configure a Sys Log for use with Filter Logs.

1 Choose Policies→Log Configuration. The Manage Log Configuration Policies form opens.

2 Perform one of the following:

a Specify SysLogTarget (Node Log Policy) and click the Search button to search for an existing Sys Log. Select a policy in the filtered list and click on the Properties button. The SysLogTarget, Global Policy (Edit) form opens with the General tab displayed.

b Click on the Create button and select Sys Log from the menu. The SysLogTarget, Global Policy (Create) form opens.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Target Description
- Target Address
- Target UDP Port
- Facility
- Severity
- Message

4 Click on the Apply button. The Policy Configuration block is displayed.

5 Click on the Switch Mode button to distribute the policy to the required NEs. A confirmation message is displayed. Click Yes. The Release - Sys Log Target form opens.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See Chapter 42 for more information.

6 Select the required NEs from the list of Available Objects on the left and move them to the Selected Objects list on the right using the right-pointing arrow.

7 Click the on the Distribute button. The Status field in the Selected Objects list provides the status of the distribution.

8 Close the Release - Sys Log Target form.

9 Close the SysLogTarget form.

10 Refer to Procedure 44-10 to associate the SysLog with a Filter Log.

Procedure 44-12 To copy filter policy filter entries

Perform this procedure to copy the filter entries of one filter policy to another filter policy. The supported filter policies include:

- ACL MAC Filter
- ACL IP Filter
- ACL IPv6 Filter
- DHCP Filter

1 Choose Policies→Filter→ Filter type from the 5620 SAM main menu, where *Filter type* is the type of filter that you want to copy a filter entry from. The appropriate policies manager form opens.

2 Click the Search button and select a policy from the list, then click the Properties button. The filter policy's properties form opens with the General tab displayed.

3 Click on the Filter Entries tab.

4 Click the Search button and select one or more filter entries from the list.

5 Click on the Copy Entries button. The Copy Filter type Filter Entries form opens and the copied filter entry appears in the Copy Policy Entry Instances panel.

6 Configure the parameters as required:

- Enable Copied Entries to Override Existing Entries with the Same ID
- Distribute the Global policy after Applying Form

7 Select the local policies that you want to copy the filter entry to from the Available Policies list. Only local policies with a distribution mode of Local Edit Only will be listed.

8 Click on the right-pointing arrow to move the selected policies to the Copy Entries to these Targeted Policies panel.



Note — If you enabled the Distribute the Global policy after Applying Form parameter and one of the Targeted Policies is a global policy, then that global policy will subsequently be distributed to all NEs with local definitions of the policy.

However, if the Distribution Mode of a local policy is set to Local Edit Only, the associated NE will not be allowed to receive the distribution of the global policy. You must set the local policy's Distribution Mode to Sync With Global if you want the NE to receive the global policy distribution.

Refer to Procedure 42-1 for detailed information on policy distribution.

9 Click on the OK button. The filter entries are copied to the targeted policies and the Copy Filter type Filter Entries form closes.



Note 1 — If you copy a filter entry with an Entry Type of Embedded, the copies sent to the targeted policies will have an Entry Type of Normal. Refer to Procedure 44-13 for information on embedded filters.

Note 2 — If an NE that contains one of the targeted policies is down, it cannot receive the copied filter. A deployment failure message will be issued.

10 Close the filter policy's properties form.

Procedure 44-13 To configure embedded and embedding filter policies

Perform this procedure to create and configure embedded and embedding filter policies. An embedded filter policy allows users to define a common set of filter policy rules that can then be nested in one or more other filter policies. The filters that support the embedded filter policies are referred to as embedding filter policies.

To create an embedded filter policy:

1 Perform one of the following procedures to create and configure the required embedded filter and its embedded filter entries. The list includes the filter policy types currently supported:

- Procedure 44-2 for ACL IP Filters
- Procedure 44-3 for ACL IPv6 Filters

When you perform any of these procedures, you must set the Scope parameter to embedded in order to create an embedded filter policy. All other steps are as stated.

The embedded filter policy will also display an Embedding Filters tab. This lists all filter policies that have been associated with this policy.

To associate an embedded filter policy with an embedding filter policy:

2 Choose Policies→Filter→ Filter type from the 5620 SAM main menu, where *Filter type* is the type of filter that you want to associate an embedded filter policy with. The supported policies include:

- ACL IP Filter
- ACL IPv6 Filter

The appropriate policies manager form opens.

3 Click the Search button and select the required policy from the list, then click the Properties button. The filter policy's properties form opens with the General tab displayed.

4 Click on the Embedded Filters tab.

5 Click the Create button. The Embedded Entry (Create) form opens.

6 Click on the Select button. The Select Embedded Filter list form opens.

7 Click the Search button and select the required embedded filter policy from the list.

8 Click OK. The Select Embedded Filter list form closes.

9 Configure the parameters:

- Offset
- Admin state

10 Click OK. The Embedded Entry (Create) form closes and the new entry is displayed in the Embedded Filters tab list.

11 A message is also displayed. Click OK to acknowledge.

12 Click on the Apply button.

13 A confirmation message is displayed. Click Yes.

14 View the properties of an embedded filter policy's filter entries if required. All filter entries for the policy are listed in the Normal Entries sub-tab under the main Filter Entries tab. The Entry Type for an embedded filter policy's filter entry will show as Embedded in the list. Regular (unembedded) filter entries will show as Normal in the list.

15 Once the embedding filter policy has been distributed, any local definitions of the global policy will display an Embedded Entries Ref Info sub-tab under the main Filter Entries tab. Use this tab if required to display additional information for the embedded filter entries only, including their Operational State (shown as Inserted, Overruled, or Inactive No Resources).

If an embedded filter entry's Operational State is shown as Overruled or Inactive No Resources, you can set the Admin State of the parent Embedded Entry (in the Embedded Filters tab) to Inactive to disable the filter entry in the local definition. If you do that, the embedded filter entry's Operational State will then show as Inactive Admin Down.

16 Click on the OK button. The filter policy's properties form closes.



Note — If you copy an embedded filter policy (Scope: embedded) using the Copy option under the More Actions button, the copied policy will also have a Scope of embedded. Embedded filter entries from the embedded policy are also copied, and will have an Entry Type of Normal. Refer to Procedure 44-12 for information on copying filter entries.

45 — Multicast policies

45.1 Multicast policies overview *45-2*

45.2 Multicast policies procedures *45-6*

45.1 Multicast policies overview

You can use the 5620 SAM to create policies that regulate the flow of multicast traffic for more efficient multicast stream management, bandwidth management, traffic forwarding, and where multicast reports are sent.

Egress multicast groups

In VPLS standard multicasting, copies of the original packets are looped back to the SAP for transmission to each destination: an activity that consumes resources and makes the handling of congestion issues more difficult.

A more efficient method of forwarding multicast packets is to group destination SAPs in a set or "chain" that receives a single multicast packet from the egress forwarding plane with only a single pass. Adding SAPs to an EMG eliminates loopbacks by forwarding a multicast packet once to a group of shared definitions. As a result, an EMG makes multicasting more efficient and more scalable.

Creating an EMG in the 5620 SAM is similar to creating a policy, because it is first created globally and then distributed to NEs. The EMG is applied to an L2 access interface that has been created on an Ethernet port with null or dot1q encapsulation. SAP membership in an EMG has the following requirements:

- The SAP must belong to an SHG.
- The L2 access interface egress ACL filter must match that of the EMG.
- The access port and the EMG must have the same encapsulation type.

When a SAP becomes a member of an EMG, the common parameters that it shares with other EMG members cannot be changed. On the other hand, a modification to an EMG common requirement changes that parameter in all SAPs in the chain. The same common required traits apply to egress filters: individual SAP filters cannot be changed, and any change to the EMG egress filter parameters affects the egress filters in all member SAPs. In addition, if an egress filter is not defined in the EMG common parameter requirements, a new member SAP cannot have an egress filter.

The following restrictions also apply to an EMG:

- only IPv4 egress filters can be applied to an EMG
- up to 30 EMGs can be created on a router
- an EMG can be deleted only if it has no SAP members
- the number of members in an EMG (the chain limit) is restricted to 30, with an optimal length of 10 to 16

Multicast package policies

Multicast package policies are also used to assign a common set of multicast groups to all 7450 ESS, 7750 SR, and 7950 XRS NEs in an MVR VPLS. Multicast package policies ensure that the multicast groups on the devices of one or more MVR VPLS instances are consistent. See chapter 22 for information about configuring multicast groups on individual devices using a multicast routing policy.

When a multicast package policy is distributed to a 7450 ESS, 7750 SR, or 7950 XRS, a multicast routing policy is configured with the appropriate multicast prefix list, which is based on the multicast groups in the multicast package policy. Multicast package policies are only used to distribute the policies to one of the two NEs. Policy discovery and synchronization are not supported.

A multicast package policy has zero or more multicast groups associated with it. The multicast groups are distributed to the 7450 ESS, 7750 SR, or 7950 XRS as part of the policy. Only root catalog multicast packages can be distributed to the 7450 ESS, 7750 SR, or 7950 XRS.

Distributing multicast package policies

When you distribute a multicast package policy to a 7450 ESS, 7750 SR, or 7950 XRS, the 5620 SAM maps one multicast package policy to one routing policy statement. Each multicast policy group entry is mapped to one routing policy prefix list member.

For example, the ID of a multicast package policy is 2. When the policy is distributed to a 7450 ESS, 7750 SR, or 7950 XRS, the 5620 SAM automatically creates a routing policy statement for the device. The name created for the routing policy statement is SAM_MPP_2, where 2 is the multicast package policy ID.

When the policy is distributed to the 7450 ESS, 7750 SR, or 7950 XRS, the ID of the routing policy statement entry is always 1. A name is generated by the 5620 SAM to identify the prefix list in the routing policy statement entry. The name is SAM_MPG_2_1, where 2 is the multicast package policy ID and 1 is the routing policy statement entry ID. The prefix list name is referenced in the routing policy statement entry as the multicast group prefix list name.

In the same example, the multicast address for the multicast group of a multicast package policy is 224.0.0.0. When the multicast package policy is distributed to a 7450 ESS, 7750 SR, or 7950 XRS, the 5620 SAM automatically creates a routing policy prefix list member for the device. The prefix list member address is 224.0.0.0.

Since the multicast package policy is not resynchronized, you must avoid duplicate names for routing policies.

For the 7450 ESS, 7750 SR, or 7950 XRS, if a multicast group does not have a policy group entry, the multicast group is not distributed to the device as a prefix member.

If a multicast package policy is used by any MVR VPLS, it cannot be removed from the 5620 SAM.

Multicast CAC policies

Multicast CAC policies control the bandwidth consumed by BTV distribution services. Bandwidth control helps manage network congestion and maintain QoS standards. The multicast CAC function is supported on any IGMP and PIM interface, IGMP group interfaces, and in the case of BTV distribution, on VPLS SAPs and SDPs where IGMP snooping is enabled.

A multicast CAC policy manages the bandwidth consumed by BTV services on both the access node link and specific links in the aggregation network. Routers in the path are configured to maintain certain limits on broadcast bandwidth and can limit the number of channels simultaneously sent on both the second mile link and the network link.

Multicast CAC policies are supported for VPLS on the 7950 XRS, 7710 SR, 7750 SR, and 7450 ESS.

Ingress Multicast Bandwidth policy

Ingress Multicast Bandwidth policies are used to manage the ingress multicast path bandwidth of the multicast forwarding paths into the switching fabric. When Multicast Path Management is disabled (the default), two paths are available:

- a high-priority path, on which packets from queues classified as “expedited” are forwarded
- a low-priority path on which packets from queues classified as “non-expedited” are forwarded

When Multicast Path Management is enabled, an Ingress Multicast Bandwidth policy can be used to manage the flow of multicast traffic through an MDA (IOM, IOM 2, or XMA) or the forwarding plane of an 2 x XP MDA IOM 3, IMM, or XCM.

The maximum number of bandwidth policies per NE is 32, including the default policy.

MDAs can be configured to use previously defined Ingress Multicast Bandwidth policies. However, any path limits specified in the selected policy can be overridden for each MDA, if required.

Ingress Multicast Info policy

Ingress Multicast Info policies are used to define how each multicast channel is handled by NEs. The policy is assigned to a VPLS/VPRN service site or default routing instance, but the policy is actually used by the Ingress Multicast Bandwidth Manager, the ECMP Path Manager, and the Egress Multicast CAC Manager to determine the path through the switch fabric and to make decisions on joins to multicast streams.

The maximum number of Info policies per NE is limited to 32, including the default policy.

MDAs can be configured to use previously-defined Ingress Multicast Bandwidth policies. However, any path limits specified in the selected policy can be overridden for each MDA, if required.

Ingress multicast forwarding on L2-snooped and L3-routed IP multicast traffic can be explicitly configured by applying an Ingress Multicast Path Management Info policy to a VPLS site (all types of VPLS are supported), a VPRN site, or the default routing instance.

An Info policy consists of one or multiple named Bundles, which in turn, contain Channel ranges with possible overrides for individual channels.

Bundles

A Bundle groups a set of explicit multicast channels (or channel ranges) into a common bandwidth context for CAC functions (such as join decisions) using common preferences. The channels in the bundle are managed as a defined percentage of the available bandwidth.

Bundles also simplify provisioning, since the default characteristics of the bundle channels are specified on the bundle level. These characteristics can be overridden at the Channel range level, or explicitly per channel.

Each Info policy has a default bundle named “default”. It cannot be edited or removed. Any multicast channel that fails to match a channel range within an explicit operator-defined bundle is associated with this default bundle.



Note — The maximum number of Bundles per Info policies is limited to 32. This limit includes the default bundle, leaving 31 operator-defined bundles per Info policy.

Channels and channel ranges

Channel ranges are used to define a set of multicast channels contained in a bundle and to override the default channel settings in the containing bundle.

A channel range is defined by a start destination multicast IP address and an end destination multicast IP address (both IP v4 and IPv6 are supported, but the start and end addresses must be of the same type). A channel in this context is a channel range where the start address and end address are identical.



Note — After you create a channel range, it is not possible to modify the start address or end address.

A channel range can contain multiple channel overrides. A channel override is used to specify an explicit setting for a channel within the range. The channel override is identified by a destination multicast IP address which falls between the start and end IP addresses of the channel range.



Note — The 7450 ESS does not support channel ranges and channel overrides having IPv6 addresses. Therefore, the 5620 SAM does not allow the creation of such channel ranges and channel overrides on local Ingress Multicast Info policies. In addition, the 5620 SAM removes any such channel ranges and channel overrides when synchronizing local Info policies with their respective global policies.

Dual stream selection

Dual stream selection support allows a single multicast stream to be duplicated into two different transmission paths. The two paths may have different transmission characteristics, such as latency and jitter. Rather than select one stream for retransmission to the client, the duplicate stream protection feature evaluates each stream packet-by-packet, selecting the packet that first arrives (and is valid) for retransmission.

Video quality monitoring

VQM to provides the functionality to analyze the quality of a video stream just prior to reaching the STB of client in a IPTV network. Statistics reports and alarms can be generated for VQM, providing operators with a view of multicast video quality at the last mile of distribution.

Ingress Multicast Reporting Destination policy

Ingress Multicast Reporting Destination policies are used to specify the destination server for the collection of multicast reports. The policies are applied to residential subscriber IGMP policies.

7210 Multipoint Bandwidth Management policy

7210 Multicast Bandwidth Management policies are used to specify the aggregate rate limit and forwarding class queue parameters for multicast traffic. The policies are applied to the 7210 SAS-X.

SSM Translate policy

Source-Specific Multicast allows the receiver of multicast packets to specify desired source addresses to the router, so that only packets originating from the specified sources are delivered. IGMP is used by the client to inform the router of the specified addresses.

The SSM Translate Policy allows you to create global sets of SSM Translate Items that can be mass-delivered to many routers at once. Every policy has one or more SSM Translate Items. When the policy is distributed, all of these items are deployed to the target base routers.

45.2 Multicast policies procedures

This section contains procedures relating to the configuration and maintenance of multicast policies.

Procedure 45-1 To create an egress multicast group policy

1 Choose Policies→Multicast→Egress Multicast Group. The Manage Egress Multicast Group Policies form opens.

2 Perform one of the following:

- **a** Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.
- **b** Click on the Create button. The Egress Multicast Group (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Destination Chain Limit

4 Click on the SAP Common Requirements tab.

5 Configure the parameters:

- Encapsulation Type
- Dot1 Q Ethertype
- QinQ Ethertype
- QinQ Fixed Tag Value

6 Click on the Select button in the Egress Filter panel to choose an egress policy. The Select Egress Filter search form opens.

7 Select an egress policy in the list and click on the OK button. The Select Egress Filter form closes and the egress policy information appears on the Egress Multicast Group (Create) form.



Note — The egress policy that you choose for this EMG must be the same as the egress policy specified for a member SAP.

8 Click on the Apply button to save the policy. The Egress Multicast Group (Create) form reappears with the General tab displayed.

9 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.



Note 1 — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

Note 2 — To associate a SAP on the device with an EMG, the access port encapsulation type on the device must be the same as the encapsulation type that you specified in step 5.

10 Close the Egress Multicast Group form. The Manage Egress Multicast Group Policies form reappears.

11 Close the Manage Egress Multicast Group Policies form.

Procedure 45-2 To configure a multicast CAC policy

1 Choose Policies→Multicast→Multicast CAC. The Manage Multicast CAC Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Multicast CAC (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Name
- Description
- Default Action

4 Click on the Apply button. The Multicast CAC (Edit) form opens with the General tab displayed.

5 Click on the Bundles tab to associate a multicast bundle with the multicast CAC policy.

6 Click on the Create button. The Multicast CAC Bundle (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Name
- Description
- Max Bandwidth (kbps)
- Administrative State

8 Click on the Channels tab.

9 Click on the Create button. The Multicast CAC Channel (Create) form opens.

10 Configure the parameters:

- Start Address
- End Address
- Bandwidth (kbps)
- Class
- Type

11 Click on the OK button. The Multicast CAC Channel (Create) form closes and a dialog box appears.

12 Click on the OK button. The Multicast CAC Bundle (Create) form lists the newly configured channel.

13 To add additional channels to the bundle, repeat steps 9 to 12.

14 Click on the OK button. A dialog box appears.

15 Click on the OK button. The Multicast CAC Bundle (Create) form closes and the Multicast CAC (Edit) form reappears with the Bundles tab displayed.

16 Click on the OK button. A dialog box appears.

17 Click on the OK button. The Multicast CAC (Edit) form closes and the Manage Multicast CAC Policies form reappears.

18 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

19 Select a policy and click on the Distribute button to manually distribute the policy to local devices.If the Distribute button is not visible, click on the More Actions button and choose Distribute. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

20 Close the Manage Multicast CAC Policies form.

Procedure 45-3 To configure an Ingress Multicast Bandwidth policy

1 Choose Policies→Multicast→Ingress Multicast Path Management. The Manage Ingress Path Management Policies form opens.

2 Select the Multicast Bandwidth Policy (multicast) from the object drop-down list.

3 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button and select Create Multicast Bandwidth Policy from the contextual menu. The Multicast Bandwidth Policy (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Name
- Description
- Falling Percent Reset (%)
- Admin BW Use Threshold (kbps)
- Percentage of Total pool (%)
- Reserved CBS (%)
- Displayed Name



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

5 Click on the T1 Paths tab. A table displays the policy definitions for the primary, secondary, and ancillary paths. Each path definition contains configurable parameters.

6 Choose one of the paths and click on the Properties button. The Bandwidth Policy Path (Create) form opens.

7 Configure the parameters:

- Path Limit (mbps)
- Committed Buffer Space (%)
- Maximum Buffer Space (%)
- High Priority Traffic (%)

8 Click on the Apply button. A dialog box appears.

9 Click on the OK button.

10 Repeat steps 6 to 9 for the remaining paths, if required.

11 Click on the T2 Paths tab. A table displays the policy definitions for the primary and secondary paths. Each path definition contains configurable parameters.

12 Choose one of the paths and click on the Properties button. The Bandwidth Policy Path (Create) form opens.

13 Configure the parameters:

- Number of Secondary T2 Paths
- Committed Buffer Space (%)
- Maximum Buffer Space (%)
- High Priority Traffic (%)

14 Click on the Apply button. A dialog box appears.

15 Click on the OK button.

16 Repeat steps 12 to 15 for the remaining path, if required.

17 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

18 Close the Multicast Bandwidth Policy form. The Manage Ingress Path Management Policies form reappears.

19 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 45-4 To configure an Ingress Multicast Information policy

1 Choose Policies→Multicast→Ingress Multicast Path Management. The Manage Ingress Path Management Policies form opens.

2 Choose Multicast Info Policy (Multicast) from the object drop-down list.

3 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button and select Create Multicast Info Policy from the contextual menu. The Multicast Info Policy (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Name
- Description



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

5 Click on the Bundles tab. All defined bundles are displayed, including the default.

6 Click the Create button. The Info Policy Bundle, Multicast Info Policy (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Name
- Description
- Congestion Priority Threshold
- ECMP Optimization Threshold
- Administrative BW (kbps)
- Preference Level
- BW Decision
- Falling Delay (seconds)
- Black Hole Rate (kbps)
- Explicit Path
- Keep Alive Timer Override (sec)

8 Click on the Video Defaults tab.

9 Configure the parameters:

- Video Group ID
- Channel Type
- Re-order Audio Interval (msec)
- FCC Server
- Min Duration (msec)
- Buffer Size
- Server
- Local Server

10 Configure the stream selection parameters, if the Stream Selection parameter is enabled for the video group.



Note — Stream selection parameters are only available if you are performing the configuration in the local policy definition. After the changes are applied to the local policy, the policy can be switched back to Sync With Global mode and the local changes made to the policy are retained. See chapter 42 for information on policy distribution modes.

i Enter a unicast IPv4 address for the Source Address parameter.

ii Click on the Select button beside the Primary Interface parameter. The Select - Multicast Path Management Bundle form opens.

iii Select an access interface and click on the OK button.

iv Click on the Select button beside the Secondary Interface parameter. The Select - Multicast Path Management Bundle form opens.



Note — The Primary Interface and Secondary Interface must be different.

v Select an access interface and click on the OK button.

11 Configure VQM if the Analyzer parameter is enabled for the video group.



Note — If VQM is not enabled for the video group, then parameters configured in the VQM Config tab will have no effect.

i Enable the Analyzer parameter in the VQM panel. The form displays the additional VQM Config tab.

ii Configure the Description parameter.

iii Click on the VQM Config tab.

iv Configure the parameters:

- Continuity Counter Error
- Unreferenced PID Error
- SCTE35 Error
- TEI Error
- TS Sync Loss Error

v In the PAT (Program Association Table) Repetition panel, configure the PAT Syntax parameter.

vi Enable the PCR Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- TOA (msec)

vii In the PCR (Program Clock Reference) Repetition panel, enable the PCR Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- TOA (msec)

viii In the PMT (Program Map Table) Repetition panel, configure the PMT Syntax Error parameter.

ix Enable the PMT Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- TOA (msec)

x In the PID panel, configure the parameters:

- Video PID Absent Interval (msec)
- Non Video PID Absent Intv (msec)

12 Click on the Tunnel Interfaces tab.

13 Click on the Select button beside the P2MP LSP Name parameter. The Select - Multicast Path Management Bundle form opens.

14 Select a Multicast Path Management Bundle and click on the OK button.

15 The Select - Multicast Path Management Bundle form closes and the information is displayed.

16 Click on the Select button beside the P2MP ID for LDP parameter. The Select LDP Tunnel Interface - Multicast Path Management Bundle form opens.

17 Select an LDP Tunnel Interface and click on the OK button.

18 The Select LDP Tunnel Interface - Multicast Path Management Bundle form closes and the information is displayed.

19 Configure the Ingress LER parameter.



Note 1 — You can configure either the P2MP LSP Name parameter or the P2MP ID for LDP parameter.

Note 2 — The Ingress LER parameter is automatically configured when the P2MP ID for LDP parameter is configured.

20 Click on the Channels tab.

21 Click the Create button. The Info Policy Channel Range, Info Policy Bundle (Create) form opens with the General tab displayed.

22 Configure the channel range parameters:

- Start Address
- End Address



Note — The 7450 ESS does not support channel ranges and channel overrides having IPv6 addresses. Therefore, the 5620 SAM does not allow the creation of such channel ranges and channel overrides on local Ingress Multicast Info policies. In addition, the 5620 SAM removes any such channel ranges and channel overrides when synchronizing local Info policies with their respective global policies.

23 Configure any required overrides of the following parameters in the Channel Defaults panel:

- Administrative BW (kbps)
- Preference Level
- BW Decision
- Falling Delay (seconds)
- Black Hole Rate (kbps)
- Explicit Path

24 Click on the Video tab.

25 Configure the parameters:

- Video Group ID
- Channel Type
- Re-order Audio Interval (msec)
- FCC Server
- Min Duration (msec)
- Buffer Size
- Server
- Local Server

26 Configure the stream selection parameters, if the Stream Selection parameter is enabled for the video group.



Note — Stream selection parameters are only available if you are performing the configuration in the local policy definition. After the changes are applied to the local policy, the policy can be switched back to Sync With Global mode and the local changes made to the policy are retained. See chapter 42 for information on policy distribution modes.

i Enter a unicast IPv4 address for the Source Address parameter.

ii Click on the Select button beside the Primary Interface parameter. The Select - Multicast Path Management Bundle form opens.

iii Select an access interface and click on the OK button.

iv Click on the Select button beside the Secondary Interface parameter. The Select - Multicast Path Management Bundle form opens.



Note — The Primary Interface and Secondary Interface must be different.

v Select an access interface and click on the OK button.

27 Configure VQM if the Analyzer parameter is enabled for the video group.



Note — If VQM is not enabled for the video group, then parameters configured in the VQM Config tab will have no effect.

i Enable the Analyzer parameter in the VQM panel. The form displays the additional VQM Config tab.

ii Configure the Description parameter.

iii Click on the VQM Config tab.

iv Configure the parameters:

- Continuity Counter Error
- Unreferenced PID Error
- SCTE35 Error
- TEI Error
- TS Sync Loss Error

v In the PAT (Program Association Table) Repetition panel, configure the PAT Syntax parameter.

vi Enable the PCR Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- TOA (msec)

vii In the PCR (Program Clock Reference) Repetition panel, enable the PCR Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- TOA (msec)

viii In the PMT (Program Map Table) Repetition panel, configure the PMT Syntax Error parameter.

ix Enable the PMT Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- TOA (msec)

x In the PID panel, configure the parameters:

- Video PID Absent Interval (msec)
- Non Video PID Absent Intv (msec)

28 Click on the Tunnel Interfaces tab.

29 Click on the Select button beside the P2MP LSP Name parameter. The Select - Multicast Path Management Channel Range form opens.

30 Select a Multicast Path Management Channel Range and click on the OK button.

31 The Select - Multicast Path Management Channel Range form closes and the information is displayed.

32 Click on the Select button beside the P2MP ID for LDP parameter. The Select LDP Tunnel Interface - Multicast Path Management Channel Range form opens.

33 Select an LDP Tunnel Interface and click on the OK button.

34 The Select LDP Tunnel Interface - Multicast Path Management Channel Range form closes and the information is displayed.

35 Configure the Ingress LER parameter.



Note 1 — You can configure either the P2MP LSP Name parameter or the P2MP ID for LDP parameter, but not both.

Note 2 — The Ingress LER parameter is automatically configured when the P2MP ID for LDP parameter is configured.

36 Click on the Channel Override tab if you need to specify overrides for explicit channels within the Channel Range.

37 Click on the Create button. The Info Policy Channel Override (Create) form opens, with the General tab displayed.

38 Enter the Source Address of the channel for which you want to specify overrides.

39 Configure any required overrides of the following parameters for the channel in the Overrides panel:

- Administrative BW (kbps)
- Preference Level
- BW Decision
- Falling Delay (seconds)
- Black Hole Rate (kbps)
- Explicit Path

40 Click on the OK button. A dialog box appears. Click OK. The channel to which you applied overrides is displayed.

41 Click on the Video tab.

42 Configure the parameters:

- Video Group ID
- Channel Type
- Re-order Audio Interval (msec)
- FCC Server
- Min Duration (msec)
- Buffer Size
- Server
- Local Server

43 Configure the stream selection parameters, if the Stream Selection parameter is enabled for the video group.



Note — Stream selection parameters are only available if you are performing the configuration in the local policy definition. After the changes are applied to the local policy, the policy can be switched back to Sync With Global mode and the local changes made to the policy are retained. See chapter 42 for information on policy distribution modes.

i Enter a unicast IPv4 address for the Source Address parameter.

ii Click on the Select button beside the Primary Interface parameter. The Select - Multicast Path Management Bundle form opens.

iii Select an access interface and click on the OK button.

iv Click on the Select button beside the Secondary Interface parameter. The Select - Multicast Path Management Bundle form opens.



Note — The Primary Interface and Secondary Interface must be different.

v Select an access interface and click on the OK button.

44 Configure VQM if the Analyzer parameter is enabled for the video group.



Note — If VQM is not enabled for the video group, then parameters configured in the VQM Config tab will have no effect.

i Enable the Analyzer parameter in the VQM panel. The form displays the additional VQM Config tab.

ii Configure the Description parameter.

iii Click on the VQM Config tab.

iv Configure the parameters:

- Continuity Counter Error
- Unreferenced PID Error
- SCTE35 Error
- TEI Error
- TS Sync Loss Error

v In the PAT (Program Association Table) Repetition panel, configure the PAT Syntax parameter.

vi Enable the PCR Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- TOA (msec)

vii In the PCR (Program Clock Reference) Repetition panel, enable the PCR Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- TOA (msec)

viii In the PMT (Program Map Table) Repetition panel, configure the PMT Syntax Error parameter.

ix Enable the PMT Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- TOA (msec)

x In the PID panel, configure the parameters:

- Video PID Absent Interval (msec)
- Non Video PID Absent Intv (msec)

45 Click on the Tunnel Interfaces tab.

46 Click on the Select button beside the P2MP LSP Name parameter. The Select - Multicast Path Management Channel Range form opens.

47 Select a Multicast Path Management Channel Range and click on the OK button.

48 The Select - Multicast Path Management Channel Range form closes and the information is displayed.

49 Click on the Select button beside the P2MP ID for LDP parameter. The Select LDP Tunnel Interface - Multicast Path Management Channel Range form opens.

50 Select an LDP Tunnel Interface and click on the OK button.

51 The Select LDP Tunnel Interface - Multicast Path Management Channel Range form closes and the information is displayed.

52 Configure the Ingress LER parameter.



Note 1 — You can configure either the P2MP LSP Name parameter or the P2MP ID for LDP parameter, but not both.

Note 2 — The Ingress LER parameter is automatically configured when the P2MP ID for LDP parameter is configured.

53 Click on the Video Interfaces tab if you need to configure a video interface.



Note — If you are configuring a video interface you must perform the configuration in the local policy definition. After the changes are applied to the local policy, the policy can be switched back to Sync With Global mode and the local changes made to the video interface are retained. See chapter 42 for information on policy distribution modes. See chapter 30 for more information about IPTV video features and configuration.

54 Click on the Create button. The Multicast Video Interface (Create) form opens with the General tab displayed.

55 Configure the Address parameter.

56 Click on the Channel Config tab.

57 Select a channel in the list and click on the Properties button. The Multicast Video Interface Channel Config (Create) form opens.

58 Configure the parameters:

- RT Rate
- Local Retransmission Server
- RT Payload Type
- FCC Server Mode
- FCC Burst
- FCC MC Handover Rate
- Max IGMP Latency
- Max Number of Sessions

59 Click on the OK button. The Multicast Video Interface Channel Config (Create) form closes and a dialog box appears.

60 Click on the OK button. The configured channels are displayed in the list.

61 Repeat steps 56 to 60 to configure additional channels, if required.

62 Click on the OK button. The Multicast Video Interface (Create) form closes and a dialog box appears.

63 Click on the OK button.

64 Click on the Apply button.

65 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

66 You can view information on VPLS sites (regular sites and I-Sites), VPRN sites, and Default Routing Instances affected by the Multicast Info Policy by clicking the appropriate tab. Run a search and view the properties for the desired item.

67 Close the Multicast Info Policy form. The Manage Ingress Path Management Policies form reappears.

68 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 45-5 To create or edit an ingress multicast reporting destination policy

1 Choose Policies→Multicast→Ingress Multicast Path Management. The Manage Ingress Path Management Policies form opens.

2 Select Multicast Reporting Destination (Multicast) from the object drop-down list.

3 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button and select Multicast Reporting Destination from the list. The Multicast Reporting Destination, Global Policy (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Name
- Description
- Destination Address
- Destination UDP Port
- Max Delay (Deciseconds)
- Administrative State

5 Click on the Apply button to save the policy. The Multicast Reporting Destination, Global Policy (Edit) form appears with the General tab displayed.

6 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

7 Close the Multicast Reporting Destination, Global Policy (edit) form.

8 Close the Ingress Path Management Policies form.

Procedure 45-6 To configure a Multicast SSM Translate policy



Note — IGMP must be enabled on the routers to which you intend to distribute the SSM Translate policy.

1 Choose Policies→Multicast→SSM Translate. The SSM Translate Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The SSM Translate Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the SSM Translate Items tab. All defined SSM Translate Items are displayed.

5 Click the Create button. The SSM Translate Policy Item (Create) form opens.

6 Configure the parameters:

- Start Mcast Address
- End Mcast Address
- Configured Source



Note — The SSM Translate Items added to a policy should not have overlapping IPv4 address ranges, otherwise a configuration error message will be issued.

7 Click OK. An information dialog box is displayed. Click OK.

8 Click the Apply button.

9 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when they are used by resources on the device.



Note 1 — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

Note 2 — When you distribute an SSM Translate policy to a router, it replaces any SSM Translate policy that may exist on that router. All existing SSM Translate Items on the router will be overwritten.

10 Close the SSM Translate Policy (Create) form. The SSM Translate Policies form reappears.

11 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 45-7 To view NE multicast reporting destination statistics

Perform this procedure to view multicast reporting destination statistics for a particular NE. This procedure allows you to display useful information including frames and records lost and sent. See “Statistics collection configuration” in the *5620 SAM Statistics Management Guide* for general information about configuring and collecting statistics.

1 Choose Policies→Multicast→Ingress Multicast Path Management. The Ingress Path Management Policies form opens.

2 Choose Local from the Policy scope drop-down menu.

3 Click on the Select button to select an NE. The Select a Network Element form opens.

4 Choose an NE in the list and click on the OK button. The NE IP address is displayed in the Local Node IP Address field.

5 Choose Multicast Reporting Destination (Multicast) from the object drop-down list.

6 Specify a filter to search for an existing policy.

7 Choose a policy from the list and click on the Properties button. The Multicast Reporting Destination, Local Policy (Edit) form opens.

8 Click on the Statistics tab.

9 Click on the Collect button to collect on-demand statistics.

10 Choose a statistics record and click on the Properties button to view the record. The Statistics Record - Multicast Reporting Destination Stats form opens.

11 View the statistics information.

12 Close the statistics record form.

13 Close other open forms, as required.

Procedure 45-8 To view multicast CAC channel statistics

Perform this procedure to view multicast CAC channel statistics and identify the status of BTV channels on a managed NE. This procedure allows you to display useful information including which channels are blocked and their location, bandwidth availability, the number of times channel requests are dropped on an interface, and the cause of the action based on the multicast CAC policy. See "Statistics collection configuration" in the *5620 SAM Statistics Management Guide* for general information about configuring and collecting statistics.

1 Choose Tools→BTV Channel Monitor. The Select Site form opens.

2 Select a site in the list and click on the OK button. The BTV Channel Monitor form opens.

3 Perform one of the following:

   a Choose Multicast CAC Channel Statistics (multicast) from the object drop-down list to list network protocol statistics.

   b Choose Multicast CAC Channel Statistics on Services (multicast) from the object drop-down list to list service statistics.

4 Configure the filter criteria and click on the Search button. A list of multicast CAC channel statistics is displayed at the bottom of the form.



Note — To get the most recent channel information on a managed NE, perform a resynchronization by clicking on the Resync button before clicking on the Search button.

5 Close the BTV Channel Monitor form.

Procedure 45-9 To configure a multicast package policy

Use multicast package policies to:

- define a set of broadcast channels that are multicast across a ring group in a BTV VLAN
- assign a common set of multicast groups to all 7450 ESS, 7750 SR, and 7950 XRS NEs in an MVR VPLS to ensure accuracy and consistency

Consider the following when creating multicast package policies:

- one root multicast package policy should be created for a ring or multiple rings, which contains the multicast addresses of all BTV channels distributed in the ring
- specify this root multicast package policy for the BTV (MVR) VLAN
- create other multicast package policies from the root package by clicking on the Copy button on the configuration form, or by clicking on the More Actions button and choosing Copy, if the Copy button is not visible.
- use the child policies to differentiate the types of broadcast TV services offered, for example, basic service and premium service

1 Choose Policies→Multicast→Multicast Package from the 5620 SAM main menu. The Multicast Package Policy Manager form opens.

2 Perform one of the following:

a Specify a filter to search for an existing policy. Select a policy in the filtered list and click on the Properties button.

b Click on the Create button. The Multicast Package Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Auto-Assign ID
- Name
- Description
- Is Root Catalogue
- IGMP Option
- Loggable

4 Click on the Multicast Groups tab.

5 Click on the Create button. The Multicast Group (Create) form opens.



Note — Each multicast group that is specified must be preconfigured in the PIM configuration. See the PIM configuration procedures in chapter 23.

6 Configure the parameters:

- Multicast Address
- Name
- Description
- Channel
- Cost

7 Click on the Apply button to save the policy. The Multicast Package Policy (Create) form is refreshed with additional buttons.

8 Click on the Distribute button to manually distribute the policy locally to devices in the ring. If the Distribute button is not visible, click on the More Actions button and choose Distribute. You can use the Distribute button when the Is Root Catalogue parameter is set to root. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

When any new devices are added to the ring, the policy is automatically distributed to any new MVR VLAN service or to any new MVR VLAN service sites in the ring.

9 Click on the Selected radio button to choose from the listed devices.

10 Choose one or more rows from the Available Nodes list.

11 Click on the right arrow button. The selected devices move to the list on the right side of the form.

12 Click on the Distribute button. The policy is distributed to the device or devices.

13 Close the Distribute form. The Multicast Package Policy form reappears.

14 Close the Multicast Package Policy form.

Create other multicast package policies from the root policy by clicking on the Copy button, as required. If the Copy button is not visible, click on the More Actions button and choose Copy. These child policies of the root policy can be used to help differentiate the types of BTV services being created, for example, basic services and premium services.

Procedure 45-10 To configure a 7210 SAS multipoint bandwidth management policy

Perform this procedure to configure a 7210 SAS multipoint bandwidth management policy. You can assign the policy to a 7210 SAS-X.

1 Choose Policies→Multicast→7210 Multipoint Bandwidth Management Policies from the 5620 SAM main menu. The 7210 Multipoint Bandwidth Management Policies form opens.

2 Perform one of the following:

   a Specify a filter to search for an existing policy. Choose a policy in the filtered list and click on the Properties button. The 7210 Multipoint Bandwidth Management (Edit) form opens with the General tab displayed.

   b Click on the Create button. The 7210 Multipoint Bandwidth Management (Create) form opens with the General tab displayed.

3 Configure the parameters:

   - Displayed Name
   - Description
   - Aggregate Rate (Mbps)

4 Click on the Queues tab. Eight default queues are displayed in the list.

5 Configure queues:

   i Choose a queue and click on the Properties button. The Multipoint Bandwidth Queue (Create) form opens.

   ii Configure the parameters:

   - ID
   - CIR (%)
   - CIR Adaptation
   - PIR (%)
   - PIR Adaptation
   - Committed Burst Size (kbps)
   - Maximum Burst Size (kbps)

   iii Click on the OK button. The Multipoint Bandwidth Queue (Create) form closes and a dialog box opens.

   iv Click on the OK button.

   v Repeat steps i to iv to configure more queues, if required.

6 Click on the OK button. A dialog box opens.

7 Click on the OK button. The 7210 Multipoint Bandwidth Management (Create) form closes.

8 Close the 7210 Multipoint Bandwidth Management Policies form.

9 Assign the policy to a 7210 SAS-X:

i Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

ii Right-click on a 7210 SAS-X and choose Properties from the contextual menu. The Network Element (Edit) form opens.

iii Click on the Globals tab.

iv Click on the Multipoint Management tab.

v Click on the Select button. The Select Bandwidth Policy form opens.

vi Configure the filter criteria, if required, and click on the Search button.

vii Choose the policy you created and click on the OK button. The Select Bandwidth Policy form closes.

10 Click on the Properties button. The 7210 Multipoint Bandwidth Management (Edit) form opens with the General tab displayed.

11 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

12 Close the 7210 Multipoint Bandwidth Management (Edit) form.

13 Close the Network Element (Edit) form.

46 — Time of day policies

46.1 Time of day policies overview *46-2*

46.2 Time of day policies procedures *46-2*

46.1 Time of day policies overview

The 5620 SAM supports the creation of time of day policies that allow you to configure time-based QoS policies, ACL filters, and schedulers that are applied to aggregation schedulers and L2 and L3 access interfaces. For example, a time of day policy allows you to manage peer-to-peer traffic by limiting access during peak hours, such as evenings and weekends.

A time range policy consists of one or more schedules, which include a start and end day and time and a priority.

A time of day suite policy is a collection of ingress and egress policies, filter policies, and schedulers, to which time range policies have been assigned. You can apply time of day suite policies to aggregation schedulers and L2 and L3 access interfaces.

You can create a time of day suite policy by assigning time range policies to the following objects to apply time and day restrictions to their deployment and access:

- ACL MAC filters and filter entries
- ACL IP filters and filter entries
- ACL IPv6 filters and filter entries
- access ingress and egress QoS policies
- scheduler policies

The default time range policy is the NO-TIME-RANGE policy, which means that no time and day restrictions apply. There can be only one NO-TIME-RANGE entry in each type of time of day suite policy entry.

Time range policies are first created globally and then distributed to NEs. You can distribute time range policies to the 7210 SAS, 7450 ESS, 7710 SR, 7705 SAR-H, 7750 SR, and 7950 XRS.

Time range assignment analysis tool

The time range assignment analysis tool allows you to view the time range policies that have been assigned over a specific time period to the following objects:

- L2 access interfaces
- L3 access interfaces
- aggregation schedulers
- time of day suite policies

You can use the time range assignment analysis tool to verify the configuration of multiple schedules and the adequacy of a time of day suite policy on a specific NE. For example, you can use this tool to verify that multiple time ranges that are assigned to IP filters in a time of day suite policy cover an entire month.

46.2 Time of day policies procedures

The following procedures describe how to configure and manage time of day policies.

Procedure 46-1 To configure a time range policy

1 Choose Policies→Time of Day→Time Range from the 5620 SAM main menu. The Time Range Policies form opens.

2 Perform one of the following:

a Specify a filter to search for an existing time range policy. Select a policy in the filtered list and click on the Properties button.

b Click on the Create button. The Time Range (Create) form opens.

3 Configure the parameters:

- Name
- Description

4 Click on the Time Range Entries tab.

5 Click on the Create button. The Time Range Entries (Create) form opens.

6 Configure the parameters:

- Start Time
- End Time
- Ongoing
- Frequency
- Start Run Day
- End Run Day

The Frequency parameter is configurable when the Ongoing parameter is enabled.

The Start Run Day and End Run Day parameters are configurable when the Frequency parameter is set to Weekly.

7 Click on the OK button. The Time Range Entries (Create) closes and a dialog box opens.

8 Click on the OK button.

9 Click on the OK button. The Time Range (Create) form closes and the Time Range Policies form reappears.

10 Click on the Search button to display the newly created policy or policies.

11 Select a policy and click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

12 Close the Manage Time Range form.

Procedure 46-2 To configure a time of day suite

Consider the following when you create a time of day suite policy:

- when there are overlapping time range policy entries within a time of day suite policy, the time range policy entry with the highest priority is applied first
- only one time of day suite policy entry without a time range (default NO-TIME-RANGE) is allowed for each type of policy
- you cannot modify a time of day suite policy entry after you create the entry
- you cannot assign the same priority of a global policy within the same policy type
- you cannot assign the same priority of a local policy within the same policy type
- you cannot assign the same time range of a global policy within the same policy type
- you cannot assign the same time range a local policy within the same policy type
- you cannot distribute a time of day suite policy entry to a local policy if the local policy already has been assigned the same time range as the global policy
- you cannot distribute a time of day suite policy entry to a local policy if the local policy already has been assigned the same priority as the global policy
- all time of day suite policy entries of a local policy are replaced by the time of day suite policy entries of a global policy if none of the entries from the local policy have the same priority or time ranges as the global policy

1 Choose Policies→Time of Day→Time Of Day Suite from the 5620 SAM main menu. The Time Of Day Suite Policies form opens.

2 Perform one of the following:

a Specify a filter to search for an existing suite. Select a suite in the filtered list and click on the Properties button.

b Click on the Create button. The Time of Day Suite (Create) form opens.

3 Configure the parameters:

- Name
- Description

4 Click on the TOD Suite Entries tab.

5 Click on the Ingress tab.

6 Assign a time range to ingress filter policies, if required. Perform the following steps:

i Click on the IP Filter, IPV6 Filter or MAC Filter tab.

ii Click on the Create button. The Ingress *type_of_filter* (Create) form opens.

iii Configure the Priority parameter.

iv Click on the Select button beside the Name parameter. The Select Time Range - Ingress *filter* list form opens.

v Select a time range in the list and click on the OK button. The Select Time Range - Ingress *filter* list form closes.

vi Click on the Select button beside the Filter ID parameter. The ingress filter list form opens.

vii Select a filter in the list and click on the OK button. The ingress filter list form closes.

viii Click on the OK button to save the configuration and close the form. The Time of Day Suite (Create) form reappears with the time of day suite entry displayed in the list.

7 Assign a time range to ingress QoS policies, if required. Perform the following:

i Click on the QoS tab.

ii Click on the Create button. The Ingress QoS (Create) form opens.

iii Configure the Priority parameter.

iv Click on the Select button in the Time Range panel. The Select Time Range - Ingress QoS list form opens.

v Select a time range in the list and click on the OK button. The Select Time Range - Ingress QoS list form closes.

vi Click on the Select button in the Policy panel. The Select Policy - Ingress QoS list form opens.

vii Select an entry in the list and click on the OK button. The Select Policy - Ingress QoS list form closes.

viii Click on the Select button in the 7210 Policy panel. The Select 7210 Policy - Ingress QoS list form opens.

ix Select an entry in the list and click on the OK button. The Select 7210 Policy - Ingress QoS list form closes.

x Click on the OK button. A dialog box appears.

xi Click on the OK button. The Time of Day Suite (Create) form reappears.

8 Assign a time range to ingress scheduler policies, if required. Perform the following:

i Click on the Scheduler tab.

ii Click on the Create button. The Ingress Scheduler (Create) form opens.

iii Configure the Priority parameter.

iv Click on the Select button beside the Name parameter. The Select Time Range - Ingress Scheduler list form opens.

v Select a time range in the list and click on the OK button. The Select Time Range - Ingress Scheduler list form closes.

vi Click on the Select button beside the Displayed Name parameter. The Select Policy Name - Ingress Scheduler list form opens.

vii Select a filter in the list and click on the OK button. The Select Policy Name - Ingress Scheduler list form closes.

viii Click on the OK button to save the configuration and close the form. The Time of Day Suite (Create) form reappears with the time of day suite entry displayed in the list.

9 Click on the Egress tab.

10 Assign a time range to egress filter policies, if required. Perform the following steps:

i Click on the IP Filter, IPV6 Filter, or MAC Filter tab.

ii Click on the Create button. The Egress *type_of_filter* (Create) form opens.

iii Configure the Priority parameter.

iv Click on the Select button beside the Name parameter. The Select Time Range - Egress *filter* list form opens.

v Select a time range in the list and click on the OK button. The Select Time Range - Egress *type_of_filter* list form closes.

vi Click on the Select button beside the Filter ID parameter. The egress filter list form opens.

vii Select a filter in the list and click on the OK button. The egress filter list form closes.

11 Assign a time range to egress QoS policies, if required. Perform the following:

i Click on the QoS tab.

ii Click on the Create button. The Egress QoS (Create) form opens.

iii Configure the Priority parameter.

iv Click on the Select button in the Time Range panel. The Select Time Range - Egress QoS list form opens.

v Select a time range in the list and click on the OK button. The Select Time Range - Egress QoS list form closes.

vi Click on the Select button in the Policy panel. The Select Policy - Egress QoS list form opens.

vii Select an entry in the list and click on the OK button. The Select Policy - Egress QoS list form closes.

12 Assign a time range to egress scheduler policies, if required. Perform the following:

i Click on the Scheduler tab.

ii Click on the Create button. The Egress Scheduler (Create) form opens.

iii Configure the Priority parameter.

iv Click on the Select button beside the Name parameter. The Select Time Range - Egress Scheduler list form opens.

v Select a time range in the list and click on the OK button. The Select Time Range - Egress Scheduler list form closes.

vi Click on the Select button beside the Displayed Name parameter. The Select Policy Name - Egress Scheduler list form opens.

vii Select a filter in the list and click on the OK button. The Select Policy Name - Egress Scheduler list form closes.

13 Click on the OK button. The Time of Day Suite (Create) form closes and the Manage Time-of-day suite form reappears.

14 Close the Time Of Day Suite Policies form.

Procedure 46-3 To perform a time range entry assignment analysis

1 Choose Tools→Time Range Entry Assignments from the 5620 SAM main menu. The Time Range Entry Assignments form opens.

2 Click on the Select button to choose a site for the analysis. The Select SAP to Analyze form opens.

3 Select a site in the list and click on the OK button.

4 Configure the Time Range Entry Container Type parameter.

5 Click on the Select button beside the Time Range Entry Container Type to choose a specific object of the container type you chose in step 4. The appropriate list form opens.

6 Configure the filter criteria.

7 Click on the Search button.

8 Double-click on an entry in the list, or select an entry and click on the OK button. The list form closes and the Time Range Entry Assignments form refreshes.

9 Configure the Search by Time Of Day Entry Type and Time Of Day Entry Policy Type parameters.

10 Configure the Start Date and End Date parameters.

11 Click on the Search button. A list of time range entries that meet the defined criteria is displayed.

12 Double-click on an entry to view information about the time range policy and time of day suite policy. The Time Range Entry Assignment: *Start Date End Date* form opens.

13 Click on the Cancel button to close the Time Range Entry Assignment: *Start Date End Date* form.

14 Close the Time Range Entry Assignments form.

47 — VRRP policies

47.1 VRRP policies overview *47-2*

47.2 VRRP policies procedures *47-3*

47.1 VRRP policies overview

VRRP priority control-policies manage VR backup router priorities. The policies override the base priority value, depending on NE events or conditions. You can configure a VRRP policy only for the non-owner VRRP instance; the same policy can be applied to IPv4 and IPv6 VRRP instances.

The main function of a VRRP priority-control policy is to define the conditions or events that affect the VR ability to communicate with outside hosts or portions of the network. When at least one of these events is true, the base priority for the VR instance is affected in one of two ways:

- an explicit value is overridden
- a value is subtracted from the sum of delta priorities

The result is the actual in-use priority for the VR instance. Any priority event may be configured as an explicit event or a delta event.

Table 47-1 describes the policy events that you can configure using the 5620 SAM.

Table 47-1 VRRP policy events

Policy Event	Description
Host unreachable	Configures a host unreachable priority-control event that monitors the ability of a host to receive an ICMP echo reply packet from a specific IP host address. A host unreachable priority-control event creates a continuous ICMP echo request (ping) probe to the specified IP address. During ping failure, the event is considered to be set. During ping success, the event is considered to be cleared.
IPv6 Host unreachable	Configures an IPv6 host unreachable priority-control event that monitors the ability of a host to receive an ICMP echo reply packet from a specific IPv6 host address. An IPv6 host unreachable priority-control event creates a continuous ICMP echo request (ping) probe to the specified IPv6 address. During ping failure, the event is considered to be set. During ping success, the event is considered to be cleared.
LAG port down	Configures a LAG priority-control event that monitors the operational state of the links and each port in the LAG. When one or more of the ports enters the operational down state, the event is considered to be set. When all ports enter an operational up state, the event is considered to be clear.
Route unknown	Configures a route unknown priority-control event that monitors the existence of a specific active IP route prefix in the routing table. Route unknown defines a link between the VRRP priority-control policy and the RTM. The RTM registers the specified route prefix as monitored by the policy. If any change (add, delete, new next hop) occurs relative to the prefix, the policy is notified and takes action according to the priority event definition.
Port Down Events	Configures an override or adjustment to the base priority value of a VRRP VR instance depending on the operational state of the event. Port Down events can only be configured on the local definitions of VRRP policies.

(1 of 2)

Policy Event	Description
Multi Chassis IPsec Non Forwarding Events	Configures an MC IPsec priority-control event that monitors the MEP state of a device. When the MEP state is down, the event is considered to be set. When the MEP state is up, the event is considered to be clear. For more information about MC IPsec, see Chapter 37.

(2 of 2)

As priority events clear in the policy, the in-use priority can eventually be restored to the base priority value.

47.2 VRRP policies procedures

The following procedures describe how to configure and manage VRRP policies.

Procedure 47-1 To configure a VRRP priority-control policy

1 Choose Policies→VRRP from the 5620 SAM main menu. The Manage VRRP Policies form opens.

2 Perform one of the following:

- **a** Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.
- **b** Click on the Create button. The VRRP Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Displayed Name
- Description
- Delta in Use Limit

4 Click on the Apply button.

5 Perform one of the following steps:

- **a** For IPv4 hosts, click on the Host Unreachable tab.
  - **i** Click on the Create button. The Host Unreachable Event (Create) form opens.
  - **ii** Configure the parameters:
    - IP Address
    - Hold Clear (seconds)
    - Hold Set (seconds)
    - Priority Type
    - Priority
    - Limit of Echo Request Failures
    - Interval for Echo Request (seconds)
    - Timeout for Echo Request (seconds)
    - Padding Size

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The Host Unreachable Event form reappears with the newly created filter entries displayed.

v Go to step i.

b For IPv6 hosts, click on the IPv6 Host Unreachable tab.

i Click on the Create button. The IPv6 Host Unreachable Event (Create) form opens.

ii Configure the parameters:

- IP Address
- Interface Name
- Hold Clear (seconds)
- Hold Set (seconds)
- Priority Type
- Priority
- Limit of Echo Request Failures
- Interval for Echo Request (seconds)
- Timeout for Echo Request (seconds)
- Padding Size

The Interface Name parameter can be configured only when the host IP Address parameter is a Link Local Address.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The IPv6 Host Unreachable Event form reappears with the newly-created filter entries displayed.

v Go to step i.

6 Perform the following to create a Lag Port Down event.

i Click on the Lag Port Down tab.

ii Click on the Create button. The Lag Port Down Event (Create) form opens with the General tab displayed.

iii Configure the parameters:

- LAG ID
- Hold Clear (seconds)
- Hold Set (seconds)

iv Click on the Number Down tab.

v Click on the Create button. The Number Down (Create) form opens with the General tab displayed.

vi Configure the parameters:

- Number of Ports Down
- Priority
- Priority Type

vii Close the Number Down (Create) form. A dialog box appears.

viii Click on the OK button.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Lag Port Down Event form reappears with the newly created filter entries displayed.

7 Perform the following to create a Route Unknown event.

i Click on the Route Unknown tab.

ii Click on the Create button. The Route Unknown (Create) form opens with the General tab displayed.

iii Configure the parameters:

- IP Address
- Mask
- Hold Clear (seconds)
- Hold Set (seconds)
- Priority
- Priority Type
- Protocol
- Less Specific

iv Click on the Next Hop tab.

v Click on the Create button.

If the IP Address parameter you specify on the General tab is an IPv4 address, the NextHop (Create) form opens; if it is an IPv6 address, the NextHopV6 (Create) form opens.

vi Configure the Interface Name parameter if the IPv6 Next Hop Address is a Link Local Address.

vii Configure the Hop Address parameter.

viii Click on the OK button. A dialog box appears.

ix Click on the OK button.

8 Perform the following to create a Multi Chassis IPsec Non Forwarding event.

i Click on the Multi Chassis IPsec Non Forwarding tab.

ii Click on the Create button. The MC IPsec Non Forwarding Event form appears.

iii Configure the parameters:

- Group ID
- Hold Clear (seconds)
- Hold Set (seconds)
- Priority
- Priority Type

iv Click on the OK button.

9 Click on the OK button. The Manage VRRP Policies form reappears.

10 Click on the Search button to display the newly created policy or policies.

11 Select a policy in the list and click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

12 Close the Manage VRRP Policies form.

48 — Auto tunnels policies

48.1 Auto tunnels policies overview *48-2*

48.2 Workflow to configure auto tunnel creation *48-5*

48.3 Auto tunnels policies procedures *48-6*

48.1 Auto tunnels policies overview

The 5620 SAM supports the creation of service tunnels for groups of NEs based on mesh, hub-and-spoke, or ring network topology. The 5620 SAM uses tunnel management policies to define the conditions for service tunnel creation. A tunnel management policy has four components:

- the group of NEs to which the policy applies and their collective role
- the tunnel specifications, for example, the tunnel type and underlying transport
- the topology specification, for example, mesh
- a tunnel template must be applied

You can specify a system-generated naming format, or you can also specify a naming prefix. The resulting name is a combination of the user-specified prefix and the ID of the tunnel.

Tunnel templates

You must create a tunnel policy using a tunnel template. You can view, but not save or reapply, a tunnel policy created using 5620 SAM releases earlier than 7.0. For example, if a new tunnel is required as a result of group member changes, the tunnel cannot be created if the policy was created using a 5620 SAM release earlier than 7.0. If such a tunnel must be deleted as a result of group member changes, the tunnel can be deleted regardless of the state of the policy.

Depending on the tunnel type selected for an auto tunnel, an SDP or LSP tunnel template can be selected. For an RSVP LSP tunnel type, one LSP template must be selected. For an RSVP SDP tunnel type, 16 LSP templates can be selected. When an LSP parent template with more than one LSP path child templates is specified, more than one LSP path is created.

A template should be configured to be deployed to a majority of the NE types. The user must validate the template and enter appropriate changes to the script before the template can be deployed in an auto tunnel policy. The parameters that can be modified, depend on the template type.

The following parameters can be modified for an SDP template:

- name
- source NE ID
- destination NE ID
- displayed name
- LDP enabled
- underlying transport
- path ID

The following parameters can be modified for an LSP template:

- name
- source NE ID
- path ID
- displayed name

- destination IP address
- destination NE ID



Note — If the policy ID value is specified by a format policy in the template, the path ID value must be set to 0.

When you execute an LSP path template in an auto tunnel policy, the following parameters are substituted with the values from the original tunnel policy:

- name
- resource ID

You can create templates from examples. Use an example as a starting point to create service or tunnel templates with or without format and range policies. When a template with format and range policies is associated with an auto tunnel rule, the format and range policies defined in the template override the name defined in the auto tunnel rule.

Class of Service

When you implement CoS, consider the following:

- To create a CoS-based SDP using RSVP, a user must apply a combination of SDP and LSP templates. An SDP tunnel template can use up to 16 LSPs. For CoS routing, 10 LSP s are required for the following: 1 for default, 1 for multicast, and 8 LSPs for different CoS routes.
- For CoS-based forwarding, at least one LSP template must be associated with the SDP. The LSP template must be specified as the default LSP template for CoS forwarding.
- When LSP templates are not specified, during non-CoS-based forwarding, the SDPs are created without LSPs attached.

Tunnel groups

A tunnel group is defined as collection of network resources, such as NEs, that perform the same role in the network; for example, the way that the designation of a port as an access or network port defines the role of the port in the network.

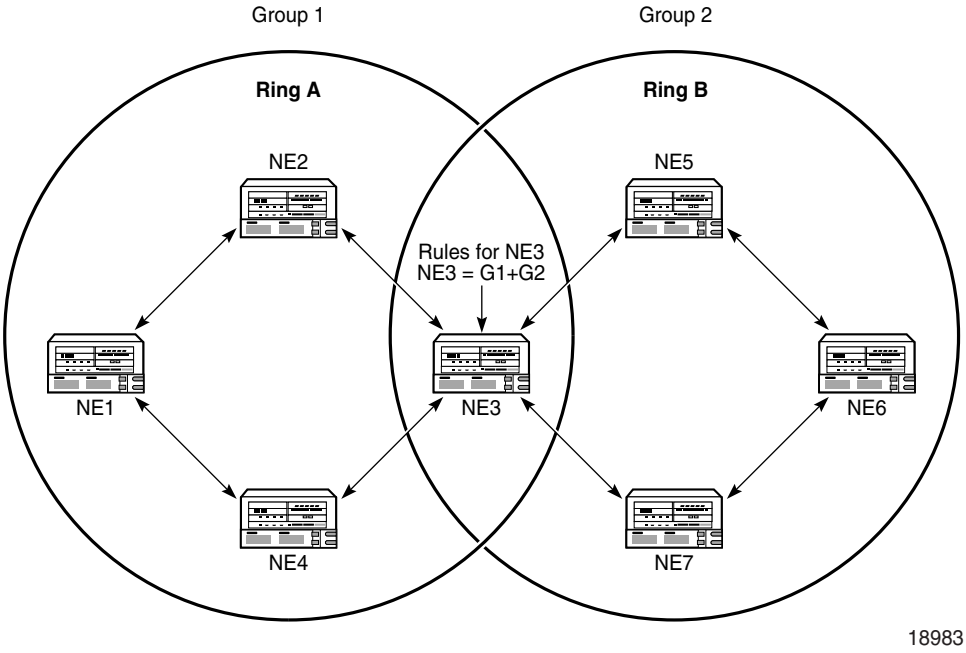
By grouping resources by role, a common policy-based management framework can be used to ensure the appropriate configuration of resources, for example, create service tunnels for different topologies.

The following conditions apply to tunnel groups.

- An NE can belong to multiple groups.
- A group is ordered or unordered depending on the requirements. The members in a group must be ordered when you create some topologies; for example, a ring topology. Topologies such as mesh or hub-and-spoke, in which NEs are not linearly arranged, do not need an ordered group.

- A non-5620 SAM-managed NE can belong to the tunnel group to which it was added, however, it is not active as a destination NE during rule execution.
- When two or more tunnel groups share an NE, the shared NE performs the roles defined for each group. In Figure 48-1, Group 1 contains routers NE1, NE2, NE3, and NE4, and Group 2 contains routers NE3, NE5, NE6, and NE7. NE3 is the intersection set of Groups 1 and 2, therefore NE3 assumes the roles defined for Groups 1 and 2.

Figure 48-1 NE shared by two tunnel groups



Tunnel policy creation requires the configuration of the following:

- one or more group conditions to specify the NEs that are included in the topology
- a least one tunnel template configuration
- one or more tunnel definitions that specify the service-tunnel characteristics, such as the type of tunnel and the underlying transport

Tunnel policy rules

The following conditions apply to tunnel policies.

- A 5620 SAM operator requires topology-management privileges to create or modify a tunnel policy.
- A tunnel can originate and terminate on 5620 SAM-managed NEs. Tunnels cannot originate on non-SAM-managed NEs, however, tunnels can terminate on non-SAM-managed NEs.
- When an NE, that is in a rule-based group, is unmanaged or delete, it is identified as unmanaged in the rule-based group. Tunnels to the NE are not removed, however tunnels from the NE are removed from 5620 SAM.

- When an auto-tunnel rule is created for a group that contains non-SAM-managed NEs, tunnels cannot be created to and from the NE using that rule.
- When you add NEs to a tunnel group that is in use, new tunnels are created according to the policy definition.
- A group condition must contain at least one group of NEs.
- Tunnel elements are not updated dynamically.
- An unmanaged NE is removed from the tunnel groups to which the NE belongs. The associated service tunnels are also removed if they originate from a managed NE. A service tunnel that originates on an unmanaged NE is retained, but is not included in the tunnel group after reconfiguration.
- When a service tunnel created by a tunnel policy is removed, the policy does not attempt to recreate the tunnel.
- You can modify the tunnel definition in a tunnel policy when the tunnel policy has not yet created a service tunnel.

Not all NEs that are assigned to a topology rule share the same functionality. The topology rule runs capability checks on the source NEs to determine whether specific tunnels or tunnel configurations can be applied. Table 48-1 lists the auto tunnel rules that are supported by each NE.

Table 48-1 Auto tunnel rules and NE support

Auto tunnel rule	7710 SR, 7450 ESS, 7750 SR, and 7950 XRS	7705 SAR
SDP LDP	X	X
SDP GRE	X	X
SDP LSP	X	X
Dynamic LSP	X	X
CoS-based SDP	X	–
LDP-over-RSVP	X	–

48.2 Workflow to configure auto tunnel creation

Perform the following steps to configure an auto tunnel.

1 Configure a tunnel template from one of the following:

- template creation form
- network or service object properties form
- pre-configured tunnel template

See “Managing templates” in the *5620 SAM Scripts and Templates Developer Guide* for more information.

2 Configure rule-based groups. See Procedure 48-1 for more information.

3 As required, convert an auto tunnel rule created using a release of the 5620 SAM earlier than release 7.0 to a template-based auto tunnel rule. See Procedure 48-2 for more information.

4 As required, configure mesh or ring topology rules. See Procedure 48-3 for more information.

5 As required, configure hub and spoke topology rules. See Procedure 48-4 for more information.

6 As required, import tunnels not managed by topology rules. See Procedure 48-5 for more information.

7 Execute a topology rule. See Procedure 48-7 for more information.

8 As required, display missing tunnel elements. See Procedure 48-8 for more information.

9 Create a service and specify Automatic Mesh SDP Binding Creation. See the appropriate service chapter for more information.

48.3 Auto tunnels policies procedures

The following procedures describe how to configure and manage auto tunnel elements.

Procedure 48-1 To create a rule-based group

1 Choose Policies→Auto Tunnels→Rule-Based Groups from the 5620 SAM main menu. The Manage Rule-Based Groups form opens.

2 Click on the Create button and choose Create Rule-Based NE Group from the menu. The Rule-Based NE Group (Create) form opens.

3 Configure the parameters.

- Group Name
- Description
- Order

4 Click on the Apply button to save the changes. The Group Members tab becomes configurable.

5 Click on the Group Members tab.

6 Depending on the value specified for the Order parameter, perform one of the following:

a Add members to an unordered group.

i Click on the Create button. The Select Network Elements form opens.

ii Select an NE and click on the OK button. A dialog box appears.

iii Click on the OK button. The Rule-Based NE Group (Edit) form reappears with the member NE displayed.

iv Repeat steps 6i to iii to add another member to the unordered group, if required or go to step 7.

b Add members to an ordered group.

i Click on the Create button. The Select Network Elements form opens.

ii Select an NE and click on the OK button. A dialog box appears.

iii Click on the OK button. The Rule-Based NE Group (Edit) form reappears with the member NE displayed.

iv Repeat steps 6i to iii to add a member to the end of the ordered group list, if required.

v To insert an NE between two NEs in the ordered group list, click on the Insert button and perform steps 6ii to iii.

7 Click the OK button. A dialog box appears.

8 Click the Yes button. The Rule-based NE Group (Edit) form closes and the Manage Rule-Based Groups form reappears.

9 Close the Manage Rule-Based Groups form.

Procedure 48-2 To convert old auto tunnel rules to template-based auto tunnel rules

Perform this procedure to convert tunnel policies created using a 5620 SAM Release earlier than 7.0 to template-based auto tunnel rules.

The number and type of templates that are displayed depend on the policy type. For example, a mesh SDP policy with GRE as the underlying transport requires 1 SDP template. A hub-and-spoke SDP policy with LSP as the underlying transport requires two SDP and two LSP templates.

When you apply a new template to an old auto tunnel rule, you must ensure that the parameter values defined in the template are consistent with the values that you defined in the original auto tunnel rule. For example, if you convert an auto tunnel rule that requires you to apply an LSP template, you must choose a template in which the LSP Bandwidth and Fast Re-Route parameter values in the template match the values defined in the old auto tunnel rule.

1 Choose Policies→Auto Tunnels→Auto Tunnel Rules from the 5620 SAM main menu. The Manage Auto Tunnel Rules form opens.

2 Click on the Search button. A list of old and new auto tunnel rules is displayed.

3 Select an old auto tunnel rule in the list.

4 Click on the Properties button. An *Auto Rule_type* (Edit) form opens.

5 Click on the Convert button. If the Convert button is not visible, click on the More Actions button and choose Convert. The Convert Old Rule form opens.



Note — The Convert option is displayed only if the selected policy has been created using a 5620 SAM Release earlier than 7.0.

6 Perform one or both of the following, depending on the type of tunnel and the underlying transport value.

When the tunnel type value is SDP and the underlying transport value is RSVP-LSP, you must choose a SDP and an LSP template. When the tunnel type value is LSP, you must choose an LSP template only.

a Click on the Select button beside the Name parameter in the SDP Template panel. The Select Template form opens.

b Click on the Select button beside the Name parameter in the LSP Template panel. The Select Template form opens.

7 Select a template in the list and click on the Execute button. The Convert Old Rule form is refreshed with the template information and the Execute button is replaced with a Done button.



Note — After an auto tunnel rule is converted, the Convert option is not displayed when the *Auto Rule_type* (Edit) form is opened.

8 Click on the Tunnel Definition tab in the *Auto Rule_type* (Edit) form. The Template panel is refreshed with the template information.

9 Close the Convert Old Rule form and close the *Auto Rule_type* (Edit) form.

Procedure 48-3 To create a mesh or ring topology rule

Perform this procedure to create a mesh topology rule for service-tunnel creation. A template must be applied to an auto-tunnel policy. You must configure an LSP or SDP tunnel template before you can deploy a template to an LSP or SDP tunnel. See "Managing templates" in the *5620 SAM Scripts and Templates Developer Guide* for information about creating tunnel templates.



Note — You must convert auto tunnel rules created using a 5620 SAM release earlier than 7.0 if the auto tunnels are not associated with a tunnel template. See Procedure 48-2 for more information.

1 Choose Policies→Auto Tunnels→Auto Tunnel Rules from the 5620 SAM main menu. The Manage Auto Tunnel Rules form opens.

2 Click on the Create button and choose one of the following:

   a Create Mesh Topology Rule. The Mesh Topology Rule (Create) form opens with the General tab displayed.

   b Create Ring Topology Rule. The Ring Topology Rule (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Name
- Description
- Naming Format
- User Specified Naming Prefix
- Template Versions
- Tunnel Creation Pacing Interval (seconds)
- Auto-Rule Execution

4 Click on the LERs Definition tab.

5 Click on the Add button. The Select Rule-Based Group form opens.

6 Click on the Search button.

7 Select a rule-based group in the list and click on the OK button. The Select Rule-Based Group form closes and the group is displayed on the Topology Rule (Create) form.

8 Click on the Tunnel Definition tab.

9 Perform one of the following to configure the Tunnel Type parameter:

   a Choose SDP.

   b Choose RSVP-LSP; go to step 19.

10 Click on the SDP tab.

11 Click on the Select button beside the Script ID parameter. The Select SDP Template form opens with a list of configured templates.

12 Select a template in the list.

13 Click on the OK button. The Select SDP Template form closes and the SDP template information is displayed on the Topology Rule (Create) form.

14 Configure the parameters:

- Underlying Transport
- Class Forwarding Capability
- Administrative State
- Import Administrative Groups

The Class Forwarding Capability and Administrative State parameters are configurable when the Underlying Transport parameter is set to RSVP-LSP.

The Administrative State parameter is not configurable when the Class Forwarding Capability parameter is disabled.

15 If you set the Underlying Transport parameter to RSVP-LSP, the LSPs tab is displayed. Click on the LSPs tab; otherwise, go to step 22.

16 Click on the Add button. The Select LSP Template form opens.

17 Select a template in the list and click on the OK button. The Select LSP Template form closes and the Topology Rule (Create) form displays the LSP template information.

18 Go to step 22.

19 Click on the Select button beside the Script ID parameter. The Select LSP Template form opens.

20 Select a template in the list and click on the OK button. The Select LSP Template form closes and the LSP template information is displayed on the Topology Rule (Create) form.

21 Configure the Enable LDP-over-RSVP parameter.

22 Click the OK button. The Topology Rule (Create) form closes and the Manage Auto Tunnel Rules form reappears.

23 Close the Manage Auto Tunnel Rules form.

Procedure 48-4 To create a hub-and-spoke topology rule



Note — You must convert auto tunnel rules created using a 5620 SAM release earlier than 7.0 if the auto tunnels are not associated with a tunnel template. See Procedure 48-2 for more information.

1 Choose Policies→Auto Tunnels→Auto Tunnel Rules from the 5620 SAM main menu. The Manage Auto Tunnel Rules form opens.

2 Click on the Create button and choose Create Hub and Spoke Topology Rule from the contextual menu. The Hub and Spoke Topology Rule (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Name
- Description
- Naming Format
- User Specified Naming Prefix
- Template Versions
- Tunnel Creation Pacing Interval (seconds)
- Auto-Rule Execution

4 Click on the Hub LERs Definition tab.

5 Click on the Add button. The Select form opens.

6 Click on the Search button. A list of rule-based groups is displayed.

7 Select a group in the list and click on the OK button. The Select form closes and the group is displayed on the Hub and Spoke Topology Rule (Create) form.

8 Click on the Spoke LERs Definition tab.

9 Click on the Add button. The Select form opens.

10 Click on the Search button. A list of rule-based groups is displayed.

11 Select a group and click on the OK button. The Select form closes and the group is displayed on the Hub and Spoke Topology Rule (Create) form.

12 Click on the Hub Tunnel Definition tab.

13 Perform one of the following to configure the Tunnel Type parameter:

a Choose SDP.

b Choose RSVP-LSP; go to step 16.

14 Click on the SDP tab.

15 Click on the Select button beside the Script ID parameter. The Select SDP Template form opens with a list of configured templates.

i Select a template in the list.

ii Click on the OK button. The Select SDP Template form closes and the SDP template information is displayed on the Hub and Spoke Topology Rule (Create) form.

iii Configure the parameters:

- Underlying Transport
- Class Forwarding Capability
- Administrative State
- Import Administrative Groups

The Class Forwarding Capability and Administrative State parameters are displayed when the Underlying Transport parameter is set to RSVP-LSP.

The Administrative State parameter is configurable when the Class Forwarding Capability parameter is enabled.

iv If you set the Underlying Transport parameter to RSVP-LSP, the LSPs tab is displayed. Click on the LSPs tab; otherwise go to step 18.

v Click on the Add button. The Select LSP Templates form opens.

vi Select a template in the list and click on the OK button. The Select LSP Templates form closes and the Associated LSP Templates panel displays the LSP template information.

vii Select the LSP template in the Associated LSP Templates panel. If the Class Forwarding Capability parameter in step 15 is enabled, the buttons in the Class Forwarding panel become enabled; otherwise, go to step 18.

viii Click on the Set as Default LSP button to specify the LSP as the default, if required.

ix Click on the Set as Multicast LSP button to specify that the LSP is a multicast LSP, if required.

x Click on the Choose a Forwarding Class button and choose a forwarding class from the contextual menu, if required.

16 Click on the LSP tab.

17 Click on the Select button beside the Script ID parameter. The Select LSP Template form opens.

i Select a template in the list and click on the OK button. The Select LSP Template form closes and the LSP template information is displayed on the Hub and Spoke Topology Rule (Create) form.

ii Configure the Enable LDP-over-RSVP parameter.

18 Click on the Spoke Tunnel Definition tab.

19 Perform one of the following to configure the Tunnel Type parameter:

a Choose SDP.

b Choose RSVP-LSP; go to step 21.

20 Perform the following steps.

i Click on the SDP tab.

ii Click on the Select button beside the Script ID parameter. The Select LSP Template form opens.

iii Select a template in the list and click on the OK button. The Select LSP Template form closes and the LSP template information is displayed on the Hub and Spoke Topology Rule (Create) form.

iv Configure the Underlying Transport parameter.

21 Perform the following steps.

i Click on the LSP tab.

ii Click on the Select button beside the Script ID parameter. The Select LSP Template form opens.

iii Select a template in the list and click on the OK button. The Select SDP Template form closes and the SDP template information is displayed on the Hub and Spoke Topology Rule (Create) form.

iv Configure the Enable LDP-over-RSVP parameter.

22 Click the OK button. The Hub and Spoke Topology Rule (Create) form closes and the Manage Auto Tunnel Rules form reappears.

23 Close the Manage Auto Tunnel Rules form.

Procedure 48-5 To import tunnels not managed by topology rules

Use this procedure to import a tunnel that is not managed by a topology rule. After you import the tunnel, the tunnel is manage by the rule. However, the rule does not enforce the source and destination IDs to match the rule group. If the imported tunnel is not part of the group, the execute button or change notifications by the group members do not apply, even though the imported tunnel is part of the rule.

1 Choose Policies→Auto Tunnels→Auto Tunnel Rules from the 5620 SAM main menu. The Manage Auto Tunnel Rules form opens.

2 Configure the filter criteria and click on the Search button. A list of auto tunnel rules is displayed.

3 Select a rule in the list and click on the Properties button. The *Topology_Rules* (Edit) form opens.

4 Click on the Created/Imported Tunnel Elements tab.

5 Click on the Import Tunnels button. The Import Tunnels form opens.

6 Perform one of the following:

a Click on the Add SDPs button. The Select SDPs form opens. Go to step 8.

b Click on the Add LSPs button. The Select LSPs form opens.

7 Click on the Search button. A list of LSPs is displayed.

i Choose one or more LSPs in the list.

ii Click on the OK button. The Select LSPs form closes and the Import Tunnels form is refreshed with the chosen LSPs. Go to step 10.

8 Click on the Search button. A list of SDPs is displayed.

i Choose one or more SDPs in the list.

ii Click on the OK button. The Select SDPs form closes and the Import Tunnels form is refreshed with the chosen SDPs.

iii Go to step 10.

9 For topology rules where the tunnel definition is SDP and the underlying transport is RSVP-LSP, you can associate the imported LSP with the LSP template to avoid unnecessary LSP creation by the rule.

i Choose an LSP from the list of imported LSPs.

ii Click on the Associate Template With Imported LSP button. The Select LSP Templates list form opens with a list of LSP templates that are associated with the rule.

The Associate Template With Imported LSP button is enabled only in SDP-LSP rules in which the creation of multiple LSPs is supported.

iii Choose an LSP template and click on the OK button. The Select LSP Templates list form closes and the Import Tunnels for reappears.

10 Click on the Import button. The Import Tunnels form closes.

11 Click on the Created/Managed Tunnel Elements tab to view the imported networks.

12 Close the *Topology_Rules* (Edit) form.

13 Close the Manage Auto Tunnel Rules form.

Procedure 48-6 To display and delete tunnel elements

1 Choose Policies→Auto Tunnels→Auto Tunnel Rules from the 5620 SAM main menu. The Manage Auto Tunnel Rules form opens.

2 Configure the filter criteria and click on the Search button. A list of service-tunnel topology rules is displayed.

3 Select a rule and click on the Properties button. The rule properties form is displayed.

4 Click on the Created/Imported Tunnel Elements tab.

5 Click on the Search button.

6 Perform one of the following actions to delete tunnel elements, as required:

   a Click on the Delete Unused button to delete tunnels that are no longer applied to a group. A dialog box appears.

   b Click on the Delete All button to delete all tunnels that are not associated with a service. A dialog box appears.

7 Click on the Yes button. The 5620 SAM deletes the elements and removes them from the list.

8 Close the rule properties form. The Manage Auto Tunnel Rules form reappears.

9 Close the Manage Auto Tunnel Rules form.

Procedure 48-7 To execute or reapply a topology rule

Perform this procedure to execute a topology rule. Executing a topology rule causes an evaluation and reapplication of the rule.



Note — The 5620 SAM supports the reapply function, except in reference to hop-less path changes. If a hop-less path changes, it may not be corrected by a reapply operation.

1 Choose Policies→Auto Tunnels→Auto Tunnel Rules from the 5620 SAM main menu. The Manage Auto Tunnel Rules form opens.

2 Select an auto tunnel rule type from the object drop-down menu.

3 Configure the filter criteria and click on the Search button. A list of service-tunnel topology rules is displayed.

4 Select a rule and click on the Properties button. The rule properties form opens.

5 Click on the Execute button. If the Execute button is not visible, click on the More Actions button and choose Execute.

6 Close the Manage Auto Tunnel Rules form.

Procedure 48-8 To display missing tunnel elements

Perform this procedure to display the missing tunnel elements. A missing tunnel element is one that the 5620 SAM is unable to create based on the specified tunnel rules, or a tunnel element that is deleted.

1 Choose Policies→Auto Tunnels→Auto Tunnel Rules from the 5620 SAM main menu. The Manage Auto Tunnel Rules form opens.

2 Configure the filter criteria and click on the Search button. A list of service-tunnel topology rules is displayed.

3 Select a rule and click on the Properties button. The rule properties form is displayed.

4 Click on the Missing Tunnel Elements tab.

5 Click on the Search button.

6 Select a missing tunnel element and click on the Properties button. The element properties form opens.

7 View the element properties.

8 Close the element properties form. The rule properties form reappears.

9 Close the rule properties form. The Manage Auto Tunnel Rules form reappears.

10 Close the Manage Auto Tunnel Rules form.

49 — AAA policies

49.1 AAA policies overview *49-2*

49.2 Workflow to configure AAA policies *49-3*

49.3 AAA policies procedures *49-3*

49.1 AAA policies overview

AAA policies provide security for network traffic on one or more NEs. You can use the 5620 SAM to create AAA policies that provide authentication, authorization, and accounting functionality.

RADIUS-based accounting policies

A RADIUS-based accounting policy is used to send accounting information to a RADIUS server.

When an NE uses a RADIUS-based accounting policy and the creation of a subscriber host invokes the policy, the NE generates an accounting-start packet that includes the policy parameters, and forwards the packet to a RADIUS server. Depending on the policy specifications, the NE also sends interim update messages that contain usage statistics. When a policy is no longer used by any subscriber host, the NE sends an accounting-stop packet that contains the final usage statistics.

A RADIUS-based accounting policy specifies the type of accounting information that is forwarded to a RADIUS server. The information is one of the following:

- per-SLA profile—forwards start, stop, and interim update messages regarding SLA profile usage
- per-host and per-SLA profile—forwards the following:
  - start, stop, and interim update messages regarding SLA profile usage
  - start and stop messages for individual host sessions
- per-host only, on Release 9.0 and later NEs—forwards start, stop, and interim update messages for each subscriber host session

See chapter 65 for information about configuring RADIUS-based accounting policies for subscriber profiles.

NAT RADIUS accounting policies

To increase logging performance (messages-per-second) and provide a reliable logging facility, a RADIUS accounting option is provided for Large Scale NAT. The configuration of a NAT RADIUS policy and its assignment to a NAT ISA group (NAT or WLAN GW) will cause the node to instruct the RADIUS user to start logging when a port-range-block is assigned to a user, or to stop logging when this block is released back into the pool.

RADIUS server policies

A RADIUS server policy is used to configure access to a group of RADIUS servers.

A maximum of five RADIUS server entries can be created under each RADIUS server policy. These RADIUS server entries must be created under the specified routing instance. For the global policy, the RADIUS server entries can be created within all base routing instances if Base routing instance is specified, or within the sites of the specified VPRN service if VPRN routing instance is specified. A RADIUS server entry cannot be created if Management routing instance is specified.

Accounting on/off groups

An accounting on/off group defines a group of RADIUS server policies for the purpose of synchronizing accounting on/off messages across all policies in the group. It establishes which policy in the group acts as the controller policy, and which policies act as monitors. The accounting on/off state of the monitor policies is set by the controller policy.

The controller/monitor designation is configured on each RADIUS server policy in the group. Only one policy in a group can be designated as the controller.

Route download policies

A route download policy provides a mechanism for an NE to download (in advance) customer-assigned subnets from a RADIUS server, so that they can be re-advertised to the corresponding routing protocols. In this manner, subscriber connections can potentially be established faster because the routes are already in place. Routing protocol churn is reduced as subscribers connect and disconnect.

Subscriber authentication policies

A subscriber authentication policy uses RADIUS authentication to grant network access to a dynamic host. These DHCP-based policies define the parameters for dynamically-created subscriber host sessions and authenticate the sessions. They can be applied to a VPLS or IES SAP, or to a VPRN or IES group interface.

You can configure a subscriber authentication policy for LLID pre-authentication. The policy is specified as a pre-authentication policy on a local user database (see Procedure 65-5).

49.2 Workflow to configure AAA policies

1. As required, configure RADIUS-based accounting policies. See Procedure 49-1 for more information.
2. As required, configure NAT RADIUS accounting policies. See Procedure 49-2 for more information.
3. As required, configure RADIUS server policies. See Procedure 49-4 for more information.
4. As required, configure an accounting on/off group. See Procedure 49-6 for more information.
5. As required, configure route download policies. See Procedure 49-7 for more information.
6. As required, configure Subscriber authentication policies. See the *5620 SAM System Administrator Guide* for more information.

49.3 AAA policies procedures

The following procedures describe how to configure and manage AAA policies.

Procedure 49-1 To configure a RADIUS-based accounting policy

Perform the following procedure to create a RADIUS-based accounting policy to send subscriber session accounting information to the RADIUS server.

1 Choose Policies→AAA Policies→RADIUS Based Accounting from the 5620 SAM main menu. The RADIUS Based Accounting Policies form opens.

2 Perform one of the following:

   a To create a RADIUS-based accounting policy, click on the Create button. The RADIUS Accounting Policy (Create) form opens.

   b To modify a RADIUS-based accounting policy, click on the Search button to display a list of RADIUS-based accounting policy entries. Choose an entry from the list and click on the Properties button. The RADIUS Accounting Policy (Edit) form opens.

3 Configure the parameters:

- Displayed Name
- Description
- Session ID Format
- RADIUS Attributes
- Use Standard Accounting Attribute
- Host Accounting Message
- Queue Instance Accounting
- Session Accounting
- Value (minutes)
- Jitter
- Set Jitter to 10% of Interval
- Port Prefix Type
- Port Prefix String
- Port Suffix Type
- Port Type
- Port Type Value
- Calling Station ID Type
- Port Binary Specification



Note — The Port Prefix Type Port Prefix String, and Port Suffix Type parameters are configurable when the NAS Port ID option is enabled for the RADIUS Attributes parameter.

The Port Type parameter is configurable when the NAS Port Type option is enabled for the RADIUS Attributes parameter.

The Port Type Value parameter is configurable when the NAS Port Type option is enabled for the RADIUS Attributes parameter, and the Port Type parameter is set to Config.

The Calling Station ID Type parameter is configurable when the Calling Station ID option is enabled for the RADIUS Attributes parameter.

The Port Binary Specification parameter is configurable when the NAS Port option is enabled for the RADIUS Attributes parameter.

You can configure any two of the Host Accounting Message, Queue Instance Accounting, and Session Accounting parameters on a RADIUS-based accounting policy.

4 Click on the Select button in the RADIUS Script Policy panel and choose a script policy from the Select Script Policy form.

5 Click on the Select button in the RADIUS Server Policy panel and choose a RADIUS server policy from the Select RADIUS Server Policy form.

6 Configure the RADIUS servers for the policy. Perform the following:

i Click on the RADIUS Servers tab.

ii Configure the parameters:

- Source Address
- Retry Attempts
- Timeout (seconds)
- Access Algorithm

iii Configure the Router Instance parameter. If you set the Router Instance parameter to VPRN, perform step iv. Otherwise, go to step v.

iv Configure a VPRN service as a virtual router instance for the RADIUS-based accounting policy. Click on the Select button in the VPRN ID panel and choose a VPRN site from the Select VPRN ID - Radius Accounting Policy list form.

v Click on the Create button. The RADIUS Server (Create) form opens.

vi Configure the parameters:

- Auto-Assign ID
- ID
- Description
- Server IP Address
- Port
- Secret Name

vii Click on the OK button. A dialog box appears.

viii Click on the OK button.

ix Repeat steps v to viii to add additional RADIUS servers, as required.

7 Click on the OK button.

8 Perform the following steps.

i Click on the Custom Record tab. The Significant Change Criteria tab is displayed.

ii Configure the Significant Change Delta parameters.

iii Configure the parameters in the Reference Queue panel:



Note 1 — You can select all options for a parameter by clicking on the Select All button beside the counters.

Note 2 — You can deselect all options for a parameter by clicking on the Deselect All button beside the counters.

- All Queues
- Ingress Counters
- Egress Counters

iv If the All Overrides parameter is enabled, go to step vi.

v Click on the Select button below the All Overrides parameter and choose a queue to monitor for the significant change from the Select Queue form.

vi Configure the parameters in the Reference Override panel:



Note 1 — You can select all options for a parameter by clicking on the Select All button beside the counters.

Note 2 — You can deselect all options for a parameter by clicking on the Deselect All button beside the counters.

- All Overrides
- Ingress Counters
- Ingress Counters

vii If you do not enable the All Overrides parameter, go to step 9.

viii Click on the Select button below the All Overrides parameter and choose an override counter to monitor for the significant change from the Select Override form.

9 Perform the following steps.

i Click on the Queue Counter Config tab.

ii Click on the Create button. The CustomQueueConfig (Create) form opens.

iii Configure the ID parameter.

iv Configure the Counters parameter in the Ingress panel.

v Configure the Counters parameter in the Egress panel.

vi Click on the OK button. A dialog box appears.

vii Click on the OK button. The Accounting Policy (Edit) form reappears.

10 Perform the following steps.

i Click on the Override Counter Config tab.

ii Click on the Create button. The CustomOverrideConfig (Create) form opens.

iii Configure the ID parameter.

iv Configure the Counters parameter in the Ingress panel.

v Configure the Counters parameter in the Egress panel.

vi Click on the OK button. A dialog box appears.

vii Click on the OK button. The Accounting Policy (Edit) form reappears.

11 Close the RADIUS Accounting Policy (Create) form. The Manage Radius Based Accounting Policies form reappears.

12 Click on the Search button to display the newly created policy or policies. Select a policy.

13 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

14 Close the Manage Radius Based Accounting Policies form.

Procedure 49-2 To configure a NAT RADIUS accounting policy

1 Choose Policies→AAA Policies→NAT RADIUS Accounting from the 5620 SAM main menu. The NAT RADIUS Accounting Policies form opens.

2 Perform one of the following:

a To create a NAT RADIUS accounting policy, click on the Create button. The NAT RADIUS Accounting Policy (Create) form opens.

b To modify a NAT RADIUS accounting policy, click on the Search button to display a list of NAT RADIUS accounting policy entries. Choose an entry from the list and click on the Properties button. The NAT RADIUS Accounting Policy (Edit) form opens.

3 Configure the parameters:

- Displayed Name
- Description
- RADIUS Attributes
- Timeout (seconds)
- Retry Attempts
- Source Address Range Start
- Source Address Range End
- Access Algorithm

4 Configure the Router Instance parameter. If you set the Router Instance parameter to VPRN, perform step 5. Otherwise, go to step 6.



Note — The Router Instance parameter is configurable on the 7450 ESS, 7710 SR, and 7750 SR.

5 Configure a VPRN service as a virtual router instance for the NAT RADIUS accounting policy. Perform the following:

i Click on the Select button in the VPRN ID panel. The Select VPRN ID - NAT RADIUS Accounting Policy list form opens.

ii Select a VPRN site in the list and click on the OK button. The Select VPRN ID - NAT RADIUS Accounting Policy list form closes and the NAT RADIUS Accounting Policy form refreshes with the VPRN service information.

6 Configure the RADIUS servers for the policy. Perform the following:

i Click on the RADIUS Servers tab.

ii Click on the Create button. The RADIUS Server (Create) form opens.

iii Configure the parameters:

- Auto-Assign ID
- ID
- Description
- Server IP Address
- Port
- Secret Name

iv Click on the OK button. A dialog box appears.

v Click on the OK button.

vi Repeat steps ii and v to add additional RADIUS servers, as required.

7 Click on the OK button.

8 Close the NAT RADIUS Accounting Policy form. The Manage NAT RADIUS Accounting Policies form reappears.

9 Click on the Search button to display the newly created policy or policies. Select a policy.

10 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

11 Close the Manage NAT RADIUS Accounting Policies form.

Procedure 49-3 To configure an L2TP RADIUS accounting policy

Perform the following procedure to create an L2TP RADIUS accounting policy to collect usage data based on either an L2TP tunnel or an L2TP session and send this data to a RADIUS server. Refer to Procedure 23-34 for information on configuring an L2TP RADIUS accounting policy on a routing instance.

1 Choose Policies→AAA Policies→L2TP RADIUS Accounting from the 5620 SAM main menu. The L2TP RADIUS Accounting Policies form opens.

2 Perform one of the following:

a To create an L2TP RADIUS accounting policy, click on the Create button. The L2TP RADIUS Accounting Policy (Create) form opens.

b To modify an L2TP RADIUS accounting policy, click on the Search button to display a list of L2TP RADIUS accounting policy entries. Choose an entry from the list and click on the Properties button. The L2TP RADIUS Accounting Policy (Edit) form opens.

3 Configure the parameters:

- Displayed Name
- Description
- Accounting Type

4 Click the Select button in the RADIUS Script Policy block and choose a RADIUS script policy from the Select RADIUS Script Policy form.

5 Configure the parameters in the RADIUS Accounting Server panel:

- Selection Algorithm
- Retry Attempts
- Source Address
- Timeout (seconds)

The Source Address parameter only appears when you are editing an existing local version of an L2TP RADIUS Accounting Policy.

6 Configure the Router Instance parameter. If you set the Router Instance parameter to VPRN, perform step 7. Otherwise, go to step 8.



Note — The Router Instance parameter is configurable on the 7450 ESS, 7710 SR, and 7750 SR.

7 Configure a VPRN service as a virtual router instance for the RADIUS-based accounting policy. Perform the following:

i Click on the Select button in the VPRN ID panel. The Select VPRN ID - Radius Accounting Policy list form opens.

ii Select a VPRN service in the list and click on the OK button. The Select VPRN ID - Radius Accounting Policy list form closes and the L2TP Radius Accounting Policy form refreshes with the VPRN service information.

8 Configure the parameters in the RADIUS Attributes panel:

- NAS Identifier
- NAS Port Type
- Definition
- Value
- NAS Port
- Binary Specification
- NAS Port ID
- Prefix Type
- Prefix
- Suffix Type



Note — The Definition and Value parameters are only configurable when the NAS Port Type option is enabled.

The Binary Specification parameter is only configurable when the NAS Port option is enabled.

The Prefix Type, Prefix, and Suffix Type parameters are only configurable when the NAS Port ID option is enabled.

9 Configure the RADIUS servers for the policy. Perform the following:

i Click on the RADIUS Servers tab.

ii Click on the Create button. The L2TP RADIUS Server (Create) form opens.

iii Configure the parameters:

- Auto-Assign ID
- ID
- Description
- Server IP Address
- Port
- Secret Name

iv Click on the OK button. The L2TP RADIUS Server (Create) form closes and a dialog box appears.

v Click on the OK button.

vi Repeat steps ii to v to add additional RADIUS servers, as required.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button.

Close the L2TP RADIUS Accounting Policy (Create) form. The L2TP RADIUS Accounting Policies form reappears.

12 Click on the Search button to display the newly-created policy.

13 Select the newly-created policy and click the Properties button. The L2TP RADIUS Accounting Policy (Edit) form appears.

14 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

15 Close the L2TP RADIUS Accounting Policy (Edit) form.

16 Close the L2TP RADIUS Accounting Policies form.

Procedure 49-4 To configure a RADIUS server policy

1 Choose Policies→AAA Policies→RADIUS Server Policies from the 5620 SAM main menu. The Manage Radius Server Policies form opens.

2 Perform one of the following:

a To create a RADIUS server policy, click on the Create button. The Radius Server Policy (Create) form opens.

b To modify a RADIUS server policy, click on the Search button to display a list of RADIUS server policy entries. Choose an entry from the list and click on the Properties button. The Radius Server Policy (Edit) form opens.

3 Configure the parameters:

- Displayed Name
- Description
- Retry Attempts
- Timeout (seconds)
- Access Algorithm
- Source Address
- Hold Down Time (seconds)

4 Configure the Router Instance parameter. If you set the Router Instance parameter to VPRN, perform the following to configure a VPRN service as a virtual router instance for the RADIUS-based accounting policy:

i Click on the Select button in the VPRN ID panel. The Select VPRN ID - Radius Server Policy list form opens.

ii Select a VPRN site in the list and click on the OK button. The Select VPRN ID - Radius Server Policy list form closes and the Radius Server Policy form refreshes with the VPRN service information.

5 In the RADIUS Accounting Interim Update panel, configure the parameters, as required:

- Minimum Interval (seconds)
- Max Interval (seconds)
- Lifetime (hours)

6 In the RADIUS Accounting Stop panel, configure the parameters, as required:

- Minimum Interval (seconds)
- Max Interval (seconds)
- Lifetime (hours)

7 Configure RADIUS scripts for the policy, as required.

i Click on the Select button next to the Accept Script field and choose a RADIUS accept script from the Select Script Policy list form.

ii Click on the Select button next to the Authentication Request Script field and choose a RADIUS authentication request script from the Select Script Policy list form.

iii Click on the Select button next to the Accounting Request Script field and choose a RADIUS accounting request script from the Select Script Policy list form.

8 Configure an accounting on/off group for the policy, if required. Perform the following:

i Click on the Accounting On/Off tab.

ii Configure the Admin State parameter. If you set the Admin State parameter to Enabled With State Change or Enabled With Monitoring, perform step iii.

iii Click on the Select button next to the Group Name field and choose an accounting on/off group from the Select Group Name form.



Note — Only one RADIUS server policy in an accounting on/off group can be configured with an Admin State parameter of Enabled With State Change.

9 Configure the RADIUS servers for the policy. Perform the following:

i Click on the RADIUS Servers tab.

ii Click on the Create button. The Server Entry (Create) form opens.

iii Configure the parameters:

- Auto-Assign ID
- ID
- Description

iv Click on the Select button in the Server Name panel. The Select Radius Server list form opens.

v Select a RADIUS server in the list and click on the OK button. The Select Radius Server list form closes and the Radius Server Policy form refreshes with the RADIUS server information.

vi Click on the OK button. A dialog box appears.

vii Click on the OK button.

viii Repeat steps ii and v to add additional RADIUS servers, as required.

10 Click on the OK button. The Radius Server Policy form closes and the Manage Radius Server Policies form reappears.

11 Click on the Search button to display the newly created policy or policies. Select a policy.

12 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

13 Close the Manage Radius Server Policies form.

Procedure 49-5 To initiate an accounting on/off message from a RADIUS server policy

Perform the following procedure to manually send an Accounting On or Accounting Off message from a RADIUS server policy. The command is enabled only on a RADIUS sever policy that is configured as the controller in an accounting on/off group. In order to perform this procedure, the RADIUS server policy must be distributed to an NE (see chapter 42).

1 Choose Policies→AAA Policies→RADIUS Server Policies from the 5620 SAM main menu. The Manage Radius Server Policies form opens.

2 Click on the Search button to display a list of RADIUS server policy entries. Choose the RADIUS server policy from which you want to send an Accounting On or Accounting Off message and click on the Properties button. The RADIUS Server Policy (Edit) form opens.

3 Click on the Send Accounting On/Off Message button. You are prompted to confirm the action.

4 Click Ok. The Accounting On/Off Operation form opens.

5 Configure the Action parameter.

6 Click OK. The Accounting On or Accounting Off message is sent.

7 Close the Accounting On/Off Operation form, the RADIUS Server Policy, Local Policy (Edit) form, and the RADIUS Server Policy, (Edit) form.

Procedure 49-6 To configure an accounting on/off group

1 Choose Policies→AAA Policies→Accounting On/Off Group from the 5620 SAM main menu. The Accounting On/Off Groups form opens.

2 Perform one of the following:

a To create an accounting on/off group, click on the Create button. The Accounting On/Off Group (Create) form opens.

b To modify an accounting on/off group, click on the Search button to display a list of accounting on/off group entries. Choose an entry from the list and click on the Properties button. The Accounting On/Off Group (Edit) form opens.

3 Configure the parameters:

- Displayed Name
- Description

4 To manage the RADIUS server policies assigned to the accounting on/off group, click on the RADIUS Server Policies tab.

The controller policy name is displayed in the Controller panel. The monitor policies are listed in the Monitors panel.

To change a controller policy to a monitor, open its Properties form and change its accounting on/off Admin State to Enabled With Monitoring (see procedure 49-4).

To change a monitor policy to a controller, open its Properties form and change its accounting on/off Admin State to Enabled With State Change (see procedure 49-4).

5 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

6 Close the Accounting On/Off Groups form.

Procedure 49-7 To configure a route download policy

In order to configure a route download policy, you must have a RADIUS server configured on each NE that is to be associated with the route download policy (see Procedure 22-7), and you must have a RADIUS server policy configured (see Procedure 49-4).

1 Choose Policies→AAA Policies→Route Download from the 5620 SAM main menu. The Route Download Policies form opens.

2 Perform one of the following:

   a To create a route download policy, click on the Create button. The Route Download Policy (Create) form opens.

   b To modify a route download policy, click on the Search button to display a list of route download policy entries. Choose an entry from the list and click on the Properties button. The Route Download Policy (Edit) form opens.

3 Configure the parameters:

- Displayed Name
- Description
- Administrative State
- Default Metric
- Default Tag
- Maximum Number of Routes
- Download Interval
- Minimum Retry Interval
- Maximum Retry Interval
- Base User Name
- Password

4 Click on the Apply button. The Route Download Policy form refreshes with additional tabs.

5 Click the Select button in the RADIUS Server Policy panel and choose a RADIUS server policy from the Select RADIUS Server Policy form.

6 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

7 Close the Route Download Policies form.

Procedure 49-8 To configure an ISA RADIUS policy

1 Choose Policies→AAA Policies→ISA RADIUS from the 5620 SAM main menu. The ISA RADIUS Policies form opens.

2 Perform one of the following:

a To create a n ISA RADIUS policy, click on the Create button. The ISA RADIUS Policy (Create) form opens.

b To modify an ISA RADIUS policy, click on the Search button to display a list of ISA RADIUS policy entries. Choose an entry from the list and click on the Properties button. The ISA RADIUS Policy (Edit) form opens.

3 Configure the parameters:

- Displayed Name
- Description
- User Name Format
- User Name Mac Format
- NAS IP Address Origin
- Authentication RADIUS Attributes
- Timeout (seconds)
- Retry Attempts
- Source Address Range Start
- Access Algorithm
- Router Instance
- Password

4 Click on the Apply button. The ISA RADIUS Policy form refreshes with additional tabs.

5 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

6 Close the ISA RADIUS Policies form.

Procedure 49-9 To force a route download on an NE

Use this procedure to force an immediate route download on an individual NE. In order to complete this procedure, you must have a route download policy configured (see Procedure 49-7.

1 Choose Policies→AAA Policies→Route Download from the 5620 SAM main menu. The Route Download Policies form opens.

2 Click on the Search button. As list of route download policies is displayed.

3 Click on the route download policy that is configured on the NE for which you want to force a route download, and click on the Properties button. The Route Download Policy (Edit) form opens with the General tab displayed.

4 Click on the Local Definitions tab and click on the Search button. A list of NEs associated with the route download policy is displayed.

5 Click on an NE in the list and click on the Properties button. The Route Download Policy - Local Policy (Edit) form opens.

6 Click on the Force Download button. The NE sends a route request to the RADIUS server.

7 Close the Route Download Policies form.

50 — 802.1x policies

50.1 802.1x policies overview *50-2*

50.2 802.1x policies procedures *50-2*

50.1 802.1x policies overview

The 5620 SAM implementation of the 802.1X protocol provides 802.1X authentication on an individual port basis.

In an 802.1X environment, a user called the supplicant requests access to an access point, called the authenticator. The authenticator forces the supplicant into an unauthorized state, forcing them to send an EAP start message.

The authenticator returns an EAP message to request the user identity. The user returns the identity, which is forwarded by the authenticator to the authentication server. The server authenticates the user and returns an accept or reject message to the authenticator.

If an accept message is received, the authenticator changes the user state to authorized and user traffic is processed.

50.2 802.1x policies procedures

The following procedures describe how to configure and manage 802.1x policies.

Procedure 50-1 To configure an 802.1X policy



Note — Before you can create an 802.1X policy, 802.1X must be enabled on the device. See Procedure 13-8 for information about enabling 802.1X.

1 Choose Policies→Ethernet→802_1x from the 5620 SAM main menu. The Manage 802_1x Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The 802_1x Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Source Address
- Administrative Status
- Description
- Retry Attempts
- Request Timeout



Note — Do not use a colon in the policy name. The 5620 SAM uses colons as separators for the object full name.

4 Click on the RADIUS Servers tab, if required. Otherwise, go to step 8.

5 Click on the Create button. The RADIUS Server (Create) form opens.

6 Configure the parameters:

- Server Index
- IP Address
- Password
- Authorization Port
- Accounting Port
- Server Type

7 Click on the OK button. The Radius Server (Create) from closes and the 802_1x Policy (Edit) form refreshes with the server information displayed in the Radius Servers tab.

8 Click on the Apply button to save the policy. The 802_1x Policy form is refreshed with additional buttons and tabs.

9 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

Policies are also automatically distributed to devices when they are used by resources on the device.

10 Close the 802_1x Policies form.

11 Close the Manage 802_1x Policies form.

51 — PBB MRP policies

51.1 PBB MRP policies overview *51-2*

51.2 Workflow to manage PBB MRP policies *51-2*

51.3 PBB MRP policies procedures *51-2*

51.1 PBB MRP policies overview

PBB MRP policies limit the scope of MMRP advertisements to a specific network domain using ISID-based filters for both the MMRP control plane and the B-VPLS data plane. A PBB MRP policy contains a configurable option to instantiate an MMRP tree and related entry only when both an MMRP declaration and registration are received on a port.

A PBB MRP policy specifies either a forward or a drop action for the Group B-MAC attributes associated with the ISIDs that are specified in the match criteria. If the scope of the policy is set to template, you can apply the PBB MRP policy to multiple B-VPLS services.

See sections "Provider Backbone Bridging in VPLS" and "MRP and MMRP support" in chapter 68 for more information.

51.2 Workflow to manage PBB MRP policies

The following workflow lists the high-level steps required to manage PBB MRP policies.

1. Create a PBB MRP policy. See Procedure 51-1.
2. Release and distribute the PBB MRP policy to NEs. See Procedure 51-1.
3. Configure MRP forwarding control on a B-site. See Procedure 68-60.
4. Configure MRP forwarding control and apply the PBB MRP policy to a B-VPLS L2 access interface, or spoke or mesh SDP binding. See Procedures 68-47 and 68-66.

51.3 PBB MRP policies procedures

The following procedures describe how to configure and manage PBB MRP policies.

Procedure 51-1 To configure a PBB MRP policy

1. Choose Policies→Ethernet→PBB MRP from the 5620 SAM main menu. The PBB MRP Policies form opens.
2. Perform one of the following:
   a. Specify a filter to search for and configure an existing policy. Choose a policy and click on the Properties button. The PBB MRP Policy (Edit) form opens with the General tab displayed.
   b. Click on the Create button. The PBB MRP Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Name
- Description
- Scope
- Default Action

4 Click on the Entries tab.

5 Click on the Create button to create entries for the policy. The PBB MRP Policy Entry (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Entry ID
- Auto-Assign ID
- Displayed Name
- Description
- Action

7 Click on the ISID Match Criteria tab.

8 Click on the Create button to specify ISID matching criteria for an entry in the policy. Multiple ISID matching criteria can be specified for each entry. The ISID Match Criteria (Create) form opens.

9 Configure the parameters:

- Low ISID
- High ISID

10 Click on the OK button. A dialog box appears.

11 Click on the OK button. The ISID match criteria entry appears in the list.

12 To add another set of criteria repeat steps 8 to 11. Otherwise, go to step 13.

13 Click on the OK button. A dialog box appears.

14 Click on the OK button.

15 Click on the Apply button.

16 Click on the General tab.

17 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

18 Close the PBB MRP Policy (Edit) form.

19 Close the PBB MRP Policies form.

52 — AOS Ethernet Service policies

52.1 AOS Ethernet Service policies overview *52-2*

52.2 AOS Ethernet Service policies procedures *52-2*

52.1 AOS Ethernet Service policies overview

This chapter describes how to configure the UNI, SAP, and custom L2 profiles associated with OmniSwitch Ethernet services.

A SAP is associated with a stacked VLAN service. A SAP profile defines values for ingress bandwidth sharing, rate limiting, customer VLAN tag processing (translate or preserve), and priority mapping (inner to outer tag or fixed value).

A UNI profile is associated with a UNI port and configures how a variety of protocol control packets are processed on the UNI port. Processing actions include Tunnel, Drop, Peer, and MAC Tunnel.

52.2 AOS Ethernet Service policies procedures

The following procedures describe how to configure AOS Ethernet Service policies.

Procedure 52-1 To configure an OmniSwitch Ethernet service UNI profile

1 Choose Policies→Ethernet→AOS Ethernet Service from the 5620 SAM main menu. The Ethernet Service Policies form opens.

2 Perform one of the following:

   a Specify a filter to search for and modify an existing UNI profile. Select a profile in the filtered list and click on the Properties button.

   b Click on the Create button and choose Create UNI Profile. The Ethernet Service UNI Profile, Global Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- STP
- GVRP
- 802.1x
- 802.3ad
- MVRP
- OAM
- UDLD
- VTP
- PVST
- UPLINK
- 802.1AB
- AMAP
- LACPMARKER
- PAGP
- CDP
- DTP
- VLAN
- Tunnel MAC



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 As required, bind the UNI profile to a custom L2 profile.

i Click on the Custom L2 Profile Binding tab.

ii Select a custom L2 profile from the list and click on the OK button.



Note — If no custom L2 profiles exist, click on the Create button. See Procedure 52-3 for more information.

5 Click on the OK button. The Ethernet Service UNI Profile, Global Policy (Create) form closes.

6 To create more UNI profiles repeat steps 2b to 5.

7 Close the Ethernet Service Policies form.

Procedure 52-2 To configure an OmniSwitch Ethernet SAP profile

1 Choose Policies→Ethernet→AOS Ethernet Service from the 5620 SAM main menu. The Ethernet Service Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing SAP profile. Select a profile in the filtered list and click on the Properties button.

b Click on the Create button and choose Create SAP Profile. The Ethernet Service SAP Profile (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Ingress Bandwidth (Mb)
- Bandwidth Sharing
- CVLAN Treatment
- Priority Mapping
- Priority



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the OK button. The Ethernet Service SAP Profile, Global Policy (Create) form closes.

5 To create more SAP profiles repeat steps 2b to 4.

6 Close the Ethernet Service Policies form.

Procedure 52-3 To configure an OmniSwitch Ethernet service custom L2 profile

Custom L2 profiles can be configured on OS 6250Ms, Release 6.6.3 or later, OS 6250SMEs with Metro licenses, OS 6450s with Metro licenses, Release 6.6.3 or later, and OS 6850Es, Release 6.4.5 R02 or later.

1 Choose Policies→Ethernet→AOS Ethernet Service from the 5620 SAM main menu. The Ethernet Service Policies form opens.

2 Perform one of the following:

- **a** Specify a filter to search for and modify an existing custom L2 profile. Select a profile in the filtered list and click on the Properties button.
- **b** Click on the Create button and choose Create Custom L2 Profile. The Custom L2 Profile, Global Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Protocol Entry Type
- Protocol Mac



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Perform one of the following:

- **a** If you set the Protocol Entry Type parameter to Ether Type, configure the Protocol Ether Type parameter.
- **b** If you set the Protocol Entry Type parameter to Ether Sub Type, configure the Protocol Ether Type and Protocol Ether Sub Type (hex) parameters.
- **c** If you set the Protocol Entry Type parameter to Mask Type, configure the Protocol Mask parameter.
- **d** If you set the Protocol Entry Type parameter to Ssap Dsap Type, configure the parameters:
  - Protocol Ssap
  - Protocol Dsap
  - Protocol Pid (hex)

5 Click on the OK button. The Custom L2 Profile, Global Policy (Create) form closes.

6 To create more custom L2 profiles repeat steps 2b to 5.

7 Close the Manage Ethernet Service Policies form.

Procedure 52-4 To clear custom L2 profile stats

1 Right-click on an OS 6250M, an OS 6250SME with Metro license, an OS 6450NE with Metro license, or an OS 6850E in the navigation tree and choose Properties from the contextual menu. The properties form for the NE opens with the General tab displayed.

2 Click on the Globals tab.

3 Click on the L2PT Clear Stats tab.

4 Configure the parameters:

- UNI Profile Clear Stats
- UNI Port Clear Stats
- NNI Port Clear Stats

5 Click on the OK button. The properties form for the NE closes.

53 — Connection profile policies

53.1 Connection profile policies overview *53-2*

53.2 Workflow to manage connection profiles *53-3*

53.3 Connection profile policies procedures *53-3*

53.1 Connection profile policies overview

You can configure an ATM-cell Apipe service with an ATM SAP type. The SAP type is an ATM connection profile name. The 5620 SAM ATM connection connection profile configures a list of VPI/VCI pairs.

You can apply a connection profile only to a SAP that is part of an Apipe VLL with a VC Type parameter that is set to ATM-cell. The ATM SAP can be on a regular port or APS port. You can apply a connection profile to any number of ATM SAPs.

Consider the following when you configure a connection profile:

- A SAP-to-SAP VLL service is not supported using ATM SAP to which a connection profile is assigned. You must configure each VPI/VCI pair into a separate SAP and create as many Apipe VLL services with the VC type ATM-vcc as required.
- You cannot configured an ATM SAP to which a connection profile is assigned on a port which is part of a MC-APS protection group.
- You cannot add an ATM SAP to which a connection profile to an Apipe VLL endpoint. The SAP cannot be configured on a MC-LAG or MC-APS port. However, this ATM SAP can be part of a VLL service which has an endpoint on a spoke SDP.

You can configure connection profile policies on the 4-port OC-3/STM-1:OC-12/STM-4 ATM MDA and on the 16-port OC-3/STM-1 ATM MDA, on the IOM3/IMM on the 7750 SR-1, 7750 SR-7, 7750 SR-12, 7750 SR-c4, 7750 SR-c4, and the 7710 SR c4 and c12.

7210 SAS VLAN ranges on Epipe SAPs

7210 SAS VLAN ranges allow you to group a range of VLAN IDs as a single entity. This allows you to provide an Epipe VLL service configuration—such as forwarding, ACL, QoS, and accounting—to the group of VLAN IDs.

You can use a connection profile to specify either a range of VLAN IDs or individual VLANs to be grouped together in a single SAP. You can configure only one range SAP in an Epipe service. The other endpoint in the Epipe service must be a Q.* SAP or a spoke SDP binding. Access SAPs that use VLAN range values are allowed only for a Dot1Q-encapsulated port or LAG. You can configure multiple connection profiles for each port or LAG, as long as the VLAN values that are specified in each profile do not overlap.

VLAN ranges are supported on the 7210 SAS-D, 7210 SAS-M, 7210 SAS-T, and 7210 SAS-X.

53.2 Workflow to manage connection profiles

The following workflow lists the high-level steps required to manage ATM connection profiles.

1 Create an ATM connection profile. See Procedure 53-1.

2 Release and distribute the ATM connection profile to NEs. See Procedure 53-1.

3 Apply the connection profile to an Apipe VLL L2 access interface. See Procedure 67-27.

53.3 Connection profile policies procedures

The following procedures describe how to configure and manage connection profile policies.

Procedure 53-1 To configure a connection profile policy

1 Choose Policies→ATM→Connection Profile from the 5620 SAM main menu. The Manage Connection Profile form opens.

2 Perform one of the following:

a Specify a filter to search for and modify a policy, and click on the Properties button. The Connection Profile (Edit) form opens with the General tab displayed.

b Click on the Create button. The Connection Profile (Create) form opens with the General tab displayed. Configure the parameters:

- Auto-Assign ID
- Connection Profile ID

3 Configure the Description parameter.

4 Perform the following to add ATM members to the connection profile.

i Click on the ATM Member tab.

ii Click on the Create button. The ATM Member (Create) form opens.

iii Configure the parameters:

- VPI
- VCI

iv Click on the OK button. The ATM Member (Create) from closes and the Connection Profile (Edit) form refreshes with the VPI and VCI information displayed in the ATM Member tab.

v Repeat steps i to iv to add additional members. You can add up to 16 members.

5 Click on the Apply button. The Connection Profile (Edit) form is refreshed with additional tabs.

6 Click on the General tab.

7 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution, which also distributes the policy to local definitions. See chapter 42 for more information.

Policies are also automatically distributed to devices when they are used by resources on the device.

8 Close the Connection Profile form.

9 Close the Manage Connection Profile form.

Procedure 53-2 To configure a VLAN range for 7210 SAS Epipe VLL service

Perform this procedure to create a connection profile to configure a range of VLAN values that you can assign to an Dot1q SAP in an Epipe VLL service.

1 Choose Policies→ATM→Connection Profile from the 5620 SAM main menu. The Manage Connection Profile form opens.

2 Perform one of the following:

a Specify a filter to search for and modify a policy, and click on the Properties button. The Connection Profile (Edit) form opens with the General tab displayed.



Note — You cannot modify a connection profile that is associated with a SAP. If you need to modify the connection profile, you must first remove the profile from all of the SAPs with which it is associated.

b Click on the Create button. The Connection Profile (Create) form opens with the General tab displayed. Configure the parameters:

- Auto-Assign ID
- Connection Profile ID

3 Configure the Description parameter.

4 Specify the list of VLAN ranges or individual VLAN IDs to be used for mapping the VLANs to the Epipe VLL SAP.

i Click on the VLAN Ranges tab.

ii Click on the Create button. The VLAN Range form opens.

iii Configure the Range parameter.

iv Click on the OK button. The VLAN Range form closes.

v Repeat steps ii to iv to create additional ranges.

5 Click on the Apply button. The Connection Profile (Edit) form is refreshed with additional tabs.

6 Click on the General tab.

7 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution, which also distributes the policy to local definitions. See chapter 42 for more information.

Policies are also automatically distributed to devices when they are used by resources on the device.

8 Close the Connection Profile form.

9 Close the Manage Connection Profile form.

54 — Residential subscriber policies

54.1 Residential subscriber policies overview ***54-2***

54.2 Residential subscriber policy management procedures ***54-8***

54.1 Residential subscriber policies overview

Residential subscriber management requires the use of policies and profiles that include the following:

- Subscriber identification policies
- Subscriber profiles
- SLA profiles
- Subscriber explicit maps
- ANCP policies
- Host lockout policies
- Host tracking policies
- Diameter policies
- PPPoE policies

See chapter 65 for information about configuring and managing residential subscribers.

Subscriber identification policies

Subscriber identification policies apply to SAPs and associate dynamic residential subscriber hosts with NE subscriber instances. Hosts that use the same subscriber identifier, called a subscriber identification string, belong to the same subscriber and receive common general HQoS and accounting treatment as defined by the customer SLA specifications in a subscriber profile. Hosts from multiple SAPs can belong to the same subscriber, but for HQoS scheduling purposes, all hosts of a subscriber must be active on the same IOM.

A subscriber identification policy includes:

- URLs for subscriber identification scripts
- subscriber profile map
- SLA profile map

Entries in the subscriber and SLA profile maps are optional and are used for the direct assignment of profiles to hosts when hosts include profile ID strings in the DHCP Option 82 field.

Default subscriber identification policy

Although the 5620 SAM is installed with no default subscriber identification policy, the user can create a subscriber identification policy and designate it as the default policy by giving it the case-sensitive name “default”.

Subscriber identification scripts

A URL in a subscriber identification policy points to the location of a subscriber identification script that an NE uses to parse DHCP option information. During initialization, an NE downloads scripts from the URLs that are specified in the applied subscriber identification policies. An NE can store a maximum of four subscriber identification policies; each policy can contain up to three scripts.

A subscriber identification script derives the mandatory subscriber ID string, as well as a DSLAM identifier and optional profile ID strings, from the DHCP option information.

The user assigns a priority to each script in a subscriber identification policy. Only the operationally enabled script with the highest priority is active. If an NE encounters an error in a script or cannot find a script at the specified location, the NE marks the URL as operationally down, raises an alarm, and attempts to use the script that is next in priority. The script-related alarms that the 5620 SAM raises against the local instance of a subscriber identification policy are:

- warning alarm when the primary URL is operationally up but a lower-priority URL is operationally down
- major alarm when the primary script is operationally down but one of the other scripts is operationally up
- critical alarm when all scripts are operationally down

A modification to a subscriber identification script or URL takes effect only after the URL is administratively disabled and then re-enabled, which causes an NE to reload the script. Replacing or modifying a subscriber identification script or a URL can be service-affecting if not done properly. To avoid a service disruption when you modify a subscriber identification script or URL, perform Procedure 65-21.

Subscriber profiles

A subscriber profile defines the aggregate HQoS and accounting characteristics for the hosts of a specific subscriber. During the creation of a subscriber profile, the user chooses ingress and egress scheduler policies that apply to all host queues of the subscriber. A subscriber profile permits the optional selection of SLA profiles to override the SLA profiles that are named in the subscriber identification policy.

A subscriber profile can be specified in the following components, which an NE searches in the order shown when it attempts to assign a subscriber profile to a host:

- subscriber explicit map
- subscriber identification policy

A subscriber requires an association with one and only one subscriber profile. If no subscriber profile is associated with a subscriber ID string or explicitly specified by a host, and there is no available default subscriber profile on an NE or on a SAP, the NE rejects the host.

A subscriber profile can include associations to the following policy types:

- ingress scheduler
- egress scheduler
- accounting
- ANCP
- NAT
- host tracking
- RADIUS accounting
- SLA profile map
- ingress QoS
- egress QoS
- HSMDA packet byte offset override
- HSMDA queue override

- ingress and egress scheduler policy parameter overrides
- ingress and egress policer control
- ingress and egress policer control overrides

The user can define a default subscriber profile for an NE or a SAP by giving it the case-sensitive name “default” during profile creation. NE and SAP default subscriber profiles apply to hosts for which a subscriber profile is unspecified in the subscriber explicit map and subscriber identification policy.

SLA profiles

An SLA profile defines the resources that an NE assigns to a particular subset of subscriber hosts, such as VoIP telephones or BTV set-top boxes. These resources include network-access and ACL policies. An SLA profile also optionally defines the maximum number of hosts that use the profile and the action taken when the number of hosts reaches the maximum.

An SLA profile can be specified in the following components, which an NE searches in the order shown when it attempts to assign an SLA profile to a host:

- subscriber explicit map
- subscriber profile
- subscriber identification policy

An SLA profile includes:

- access ingress policy association
- access egress policy association
- ingress IP ACL filter policy association
- egress IP ACL filter policy association
- host limit that specifies the maximum number of hosts that use the SLA profile
- access ingress and access egress policy parameter override values
- access ingress and access egress policer override values

The queues in the access ingress and egress policies of an SLA profile must use a scheduler from the scheduler policy in the subscriber profile as their parent scheduler. All hosts that use the SLA profile must be active on the same IOM. When an SLA profile does not name an access ingress or access egress policy, an NE uses the SAP default policy.

The user can define a default SLA profile for a SAP. A default SAP SLA profile applies only to hosts for which an SLA profile is unspecified in the subscriber explicit map, subscriber profile, and subscriber identification policy.

Subscriber explicit maps

A subscriber explicit map is a table that directly associates dynamic subscriber hosts with subscriber profiles and SLA profiles. The entries in a subscriber explicit map override the default profile definitions. A subscriber ID string is the unique key for a subscriber explicit map entry.

A subscriber explicit map includes:

- subscriber ID string
- subscriber profile name
- SLA profile name
- AA group policy name
- subscriber ID alias

A subscriber explicit map does not allow the association of a subscriber ID string with the subscriber profile called “default”. However, if the explicit mapping omits a subscriber profile, the subscriber ID string is associated with the SAP or NE default subscriber profile. An attempt to delete a subscriber profile that is named in a subscriber explicit map fails. The user can remove explicit map entries at any time.

If the user creates a subscriber explicit map entry without using the 5620 SAM, for example, using CLI, the 5620 SAM creates a subscriber instance in the global subscriber explicit map. If the 5620 SAM subsequently discovers another NE with the same subscriber entry that has a mapping to different profile, the 5620 SAM treats the second mapping as a local mismatch to the global entry for the subscriber.

ANCP policies

An ANCP policy defines the behavior of the residential subscriber host with which the policy is associated. An ANCP policy includes one of the following:

- static ANCP association
- static ANCP MSS association
- dynamic subscriber-profile association on VPLS, IES, VPRN and VLL services

An ANCP policy conveys status and control information based on port-up/port-down messages and changes to the current access line rate between the edge device and the access node. This allows the 7450 ESS, the 7750 SR, or the 7710 SR to adjust the HQoS subscriber scheduler with the correct rate or raises an alarm when the rate goes below a set threshold. The policy can be changed if the rate drops below a minimal threshold value. The ANCP actual upstream synchronization rate is configured in the ingress panel while the ANCP actual downstream synchronization rate is configured in the egress panel.

Host lockout policies

A host lockout policy implements the ability to hold off a misconfigured or malicious subscriber that is continuously retrying to connect. This conserves resources on the NE and on the RADIUS server.

A host lockout policy can be associated with the following objects:

- VPLS or MVPLS L2 access interface
- IES or VPRN L3 access interface
- IES or VPRN group interface

Host lockouts can be cleared at the policy level, at the NE level, or from the SAP to which they are applied.

Host tracking policies

A host tracking policy is used to allow a subscriber's video traffic (multicast) to be included in the egress rate control for the subscriber. When a host tracking policy is specified in a subscriber profile, the egress traffic rate for the subscriber takes into account the unicast and multicast traffic in the aggregate egress rate or in the egress scheduler rate specified in the ANCP policy. There is no default host tracking policy.

When a host tracking policy is applied to a subscriber profile, all subscribers associated with the subscriber profile are tracked using that host tracking policy. You can view the tracked subscribers on the associated local host tracking policy property form.

You can also configure IGMP host tracking parameters on VPLS, IES, and VPRN service sites and SAPs.

The following on-demand host tracking information is available:

- on the Residential Subscriber Instance form, Host Tracking Info tab, which hosts are being tracked for this particular subscriber
- on the Residential Subscriber Instance form, Host Tracking Status tab, the egress traffic rate reduction for this particular subscriber
- on the VPLS L2 access interface property form, Host Tracking Info tab, which hosts are being tracked
- on the IES and VPRN service access point property form, Host Tracking Info tab, which hosts are being tracked

On-demand historical and real-time host tracking statistics are supported for SAPs and residential subscribers. Only historical statistical plotting is supported. The statistics and read-only host tracking information can be cleared by the 5620 SAM.

Operational states of primary and secondary RADIUS scripts

When the Up state is selected for primary or secondary scripts, the NE downloads the Python script from the specified path and copies it to the memory. If the path is invalid or the script is too long or contains syntax errors, the operational state of the script will change to the Down state. If the Python script installs correctly, the operational state of the script will remain in the Up state.

Script modifications are only applied by the NE after the script admin state has been changed to Down and then Up again.

Diameter policies

The 5620 SAM supports diameter policies and associated diameter peers. Diameter policies are used in a subscriber management context to provide a credit control mechanism. The diameter policy establishes a server/peer configuration, as well as Diameter Credit-Control Application (DCCA) support. The NE functions as the credit control client, while the peer acts as the credit control server.

DCCA represents an alternative to RADIUS for providing a mechanism to support pre-paid service model in access networks. Under a DCCA configuration, the credit control server is used to grant service to a subscriber for pre-defined duration. Before a subscriber host is created, the BNG queries the credit control server about the credit for the given subscriber. If credit is granted, the subscriber host is installed with the appropriate SLA level. If the subscriber has no credit, the credit control server denies access and no subscriber host is created.

The diameter policy is used to specify common diameter protocol parameters, while the diameter peer defines the relationship with an external diameter server. The diameter protocol parameters defined on the diameter policy describe connection and session characteristics, and indicate which AVPs to use in messages.

Peers

The diameter policy defines a set of peers with which to establish diameter sessions. Peers share the configuration of the policy with which they are associated, but can override individual timer parameters inherited from the policy. In addition, each peer defines transport and connection-specific parameters, values for destination-specific AVPs, and a preference value.

The 7750 SR and 7450 ESS provide read-only operational values and statistics for the peer definition of local diameter policies. The 5620 SAM can provide a snapshot view of operational values and statistics. Operational values include the peer's timer values, the current state of the peer's state machine, and the peer's order among the other peers within the policy.

DCCA

The 7710 SR and 7750 SR support a DCCA, which can be customized through a set of parameters on the diameter policy in the 5620 SAM. The parameters allow customization of DCCA error handling, DCCA timer(s), and AVP value definitions.

PPPoE policies

PPPoE is used in subscriber networks to encapsulate PPP frames inside Ethernet frames. PPPoE combines the point-to-point protocol used with DSL sessions with the Ethernet protocol used to support multiple subscribers in a local area network. PPPoE takes advantage of the speed of a packet-based Ethernet network with the security and accounting functions of a PPP network. PPPoE allows service providers to use existing RADIUS authentication.

Since more than one subscriber is sharing the same connection to a service provider, PPPoE organizes subscribers during two stages:

- PPPoE discovery stage
- PPPoE session stage

During the discovery stage, the subscriber and service provider identify each other’s MAC address and establish a PPPoE session ID.

The PPPoE discovery stage consists of the following steps:

1 PPPoE Active Discovery Initiation (PADI). The client initiates a session by broadcasting a PADI packet to the LAN to request a service.

2 PPPoE Active Discovery Offer (PADO). Any access device that can deliver the service requested by PADI packet, replies with a PADO packet that contains its name, unicast address and service requested.

3 PPPoE Active Discovery Request (PADR).The client selects one of the PADOs that it receives and sends a PADR packet to indicate the services required.

4 PPPoE Active Discovery Session Confirmation (PADS). When the selected device receives the PADR packet, it can accept or reject the PPPoE session. To accept the session the device sends the client a PADS packet with a unique ID and a service name. If the device rejects the session, it sends a PADS packet with a service name error and resets the session ID to zero.

During the session stage, PPPoE behaves as a peer-to-peer protocol. Each PPPoE session is identified by the MAC address of the peer and the session ID. Once a session is established, both end points build a point to point connection over the Ethernet and exchange packets. Once the connect is established, the RADIUS accounting policy can begin. LCP negotiates authentication parameters. After a session is authenticated IPCP sends an IP address to the PPPoE client. IP Addresses can be stored in the DHCP local user database, if configured.

After a session is established both end points monitor the session and can terminate a session after a configured number of keep alive intervals are exceeded. An alarm is raised by the 5620 SAM when a PPPoE session fails. Either peer can send a PPPoE Active Discovery Termination (PADT) packet. See "Local DHCP server" in this chapter for more information on associating PPPoE with a local DHCP server.

PPPoA sessions

PPPoA is used in subscriber networks to encapsulate PPP frames inside ATM Adaption Layer 5 packets. Each PPP session is carried over a single ATM VC to the BNG. Two types of encapsulation are supported:

- AAL5_nlpid_PPP
- AAL5_Mux_PPP

PPPoEoA sessions

PPPoEoA is used in subscriber networks to encapsulate PPPoE messaging within ATM Adaption Layer 5 packets. Each PPP session can be directly terminated on any host within the customer Ethernet network and then transported over an ATM network to the BNG. Two types of encapsulation are supported:

- AAL5_muxed_bridged_EHT_no_FCS
- AAL5_snap_bridged

54.2 Residential subscriber policy management procedures

Use the following procedures to perform residential subscriber policy management tasks.

Procedure 54-1 To configure a subscriber identification policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Perform one of the following.

a Create a subscriber identification policy.

i Click on the Create button and choose Create Subscriber Identification Policy from the drop-down menu. The Subscriber Identification Policy (Create) form opens.

ii Go to step 3.

b Modify a subscriber identification policy.



Caution — Modifying an active subscriber identification policy is potentially service-affecting. Ensure that you consider the implications of reconfiguring the subscriber identification policy before you proceed.

i Choose Subscriber Identification Policy from the object drop-down list.

ii Configure the filter criteria and click on the Search button. A list of subscriber identification policies appears.

iii Select a subscriber identification policy and click on the Properties button. The Subscriber Identification Policy (Edit) form opens.

3 Configure the parameters:

- Displayed Name
- Description
- Strings From Option
- Primary Script URL
- Primary Script Administrative State
- Secondary Script URL
- Remove oldest Subscriber Host
- Tertiary Script URL
- Tertiary Script Administrative State



Note 1 — You can designate a subscriber identification policy as the default policy by specifying the case-sensitive name “default” for the Displayed Name parameter. The Displayed Name parameter is configurable only during subscriber identification policy creation.

Note 2 — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Supported Service Models tab to indicate the intended service model for the subscriber identification policy.



Note — The 5750 SSC requires the specification of a service model for proper interoperation with the 5620 SAM.

5 Configure the parameters:

- VLAN per Subscriber (Routed)
- VLAN per Service (Routed)
- VLAN for all Services (Routed)
- VLAN per ISP per Service (Routed)
- VLAN per Subscriber (Bridged)
- VLAN per Service (Bridged)
- VLAN for all Services (Routed)
- VLAN per ISP per Service (Bridged)

6 Click on the SLA Profiles tab. The General tab is displayed.

7 Configure the Use Direct Map as Default parameter.

8 Perform one of the following steps to configure SLA profiles for the subscriber identification policy, if required.

a Assign an SLA profile.

i Click on the Create button. The SLAProfileEntry (Create) form opens.

ii Click on the Select button to choose an SLA profile. The Select SLA Profile form opens.

iii Select an SLA profile and click on the OK button. The Select SLA Profile form closes, and the SLAProfileEntry (Create) form refreshes with the SLA profile information.

iv Configure the SLA Profile String parameter.

v Click on the OK button to close the SLAProfileEntry (Create) form. A dialog box appears.

vi Click on the OK button. The Subscriber Identification Policy (Create) form refreshes with the SLA profile entry.

b Remove an SLA profile.

i Select an SLA profile and click on the Delete button. A dialog box appears.

ii Click on the OK button. The SLA profile is removed from the list.

iii If you want to assign an SLA profile to replace the removed SLA profile, go to step 8 a.

9 Click on the Subscriber Profiles tab. The General tab is displayed.

10 Configure the Use Direct Map as Default parameter.

11 Perform one of the following steps to configure subscriber profiles for the subscriber identification policy, if required.

a Add a subscriber profile.

i Click on the Create button. The SubscrProfileEntry (Create) form opens.

ii Click on the Select button to choose a subscriber profile. The Select Subscriber Profile form opens.

iii Select a subscriber profile and click on the OK button. The Select Subscriber Profile form closes, and the SubscrProfileEntry (Create) form refreshes with the subscriber profile information.

iv Configure the Subscriber ID Alias parameter.

v Click on the OK button to close the SubscrProfileEntry (Create) form. A dialog box appears.

vi Click on the OK button. The Subscriber Identification Policy (Create) form refreshes with the subscriber profile entry.

b Remove a subscriber profile.

i Select a subscriber profile and click on the Delete button. A dialog box appears.

ii Click on the OK button. The subscriber profile is removed from the list.

12 Click on the Application Profiles tab. The General tab is displayed.

13 Configure the Use Direct Map as Default parameter.

14 Perform one of the following steps to configure application profiles for the subscriber identification policy, if required.

a Add an application profile.

i Click on the Create button. The AppProfileEntry (Create) form opens.

ii Click on the Select button to choose an application profile. The Select Application Profile form opens.



Note 1 — If the subscriber identification policy opened in step 2 is a global policy, global AA group policies are listed. If the subscriber identification policy is a local policy, local AA group policies are listed.

Note 2 — The global AA group policies must be manually distributed to the NE before a global subscriber identification policy using the application profiles can be distributed.

Note 3 — When a new subscriber identification or subscriber explicit map is discovered from the NE, the AA group policy is not automatically resynchronized to the global subscriber identification policy.

iii Select an application profile and click on the OK button. The Select Application Profile form closes, and the AppProfileEntry (Create) form refreshes with the application profile information.

iv Configure the Application Profile parameter.

v Click on the OK button to close the AppProfileEntry (Create) form. A dialog box appears.

vi Click on the OK button. The Subscriber Identification Policy (Create) form refreshes with the application profile entry.

b Remove an application profile.

i Select an application profile and click on the Delete button. A dialog box appears.

ii Click on the OK button. The application profile is removed from the list.

15 Click on the OK button to close the Subscriber Identification Policy (Create) form. A dialog box appears.

16 To distribute the policy to an NE, if a local definition does not exist, click on the Local Definitions tab. A list of NEs appears. See Procedure 42-1 for more information about distributing a policy.

17 Click on the Yes button. The Subscriber Identification Policy (Create) form closes.

Procedure 54-2 To configure an ANCP policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Perform one of the following:

a Create an ANCP policy.

i Click on the Create button and choose Create ANCP Policy from the drop-down menu. The ANCP (Create) form opens.

ii Go to step 3.

b Modify an ANCP policy.

i Choose an ANCP policy from the object drop-down list of the Manage Subscriber Policies form.

ii Configure the filter criteria and click on the Search button. A list of ANCP policies appears.

iii Select an ANCP policy and click on the Properties button. The ANCP Policy (Edit) form opens.

3 Configure the Displayed Name parameter.



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Configure the following parameters in the Ingress panel:

- Rate Adjustment
- Rate Reduction (kbps)
- Rate Monitor (kbps)
- Rate Modification
- Rate Monitor Notification
- Rate Modification Scheduler

The Rate Modification Scheduler parameter is configurable when the Rate Modification parameter is set to Scheduler.

5 Configure the following parameters in the Egress panel:

- Rate Adjustment
- Rate Reduction (kbps)
- Rate Monitor Notification
- Rate Modification
- Rate Monitor Notification
- Rate Modification Scheduler

The Rate Modification Scheduler parameter is configurable when the Rate Modification parameter is set to Scheduler.

6 Configure the following parameters in the Port Down panel:

- Disable SHCV
- Disable SHCV Notification
- Disable SHCV Hold Time (seconds)

7 To distribute the policy to an NE. See Procedure 42-1 for more information about distributing a policy.

8 Click on the OK button to close the ANCP Policy (Create) form.

Procedure 54-3 To configure a PPPoE policy

The 5620 SAM supports PPPoE configuration on the 7750 SR and the 7710 SR.

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Choose PPPoE Policy (pppoe) from the object drop-down list in the Manage Subscriber Policies form.

3 Perform one of the following:

a Create a PPPoE policy.

i Click on the Create button. A drop down menu appears.

ii Choose Create PPPoE Policy. The PPPoE Policy, Global Policy (Create) form opens.

b Modify a PPPoE policy.

i Configure the filter criteria and click on the Search button. A list of PPPoE policies appears.

ii Select a PPPoE policy and click on the Properties button. The PPPoE Policy (Edit) form opens.

4 Configure the parameters:

- Displayed Name
- Description
- PPP MTU (octets)
- LCP Keep-Alive Interval (seconds)
- LCP Keep-Alive Hold Up Multiplier
- Disable AC Cookies
- PADO Delay (100s of milliseconds)
- Maximum Sessions Per MAC
- Enable Reply On PADT
- Authentication Type
- Minimum CHAP Challenge Length
- Maximum CHAP Challenge Length
- Initial Delay (10s of milliseconds)
- IPCP Subnet Negotiation



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

5 Click on the Apply button. The PPPoE Policy (Edit) form refreshes with the policy configuration mode information.

6 Click on the Options tab. A list of options appears.

7 Perform one of the following:

a To add an option, go to step 11.

b To edit an existing option, go to step 8.

8 Choose an option from the list.

9 Click on the Properties button. The PPPoE Option (Edit) form opens.

10 Go to step 12.

11 Click on the Create button. The PPPoE Option (Create) form opens.

12 Configure the parameters:

- Option Protocol
- Custom Option Number
- Option Type
- Option Value
- IP Address

13 Click on the OK button to close the PPPoE Option (Create) form. A dialog box appears.

14 To distribute the policy to an NE, if a local definition does not exist, click on the Local Definitions tab. A list of NEs appears. See Procedure 42-1 for more information about distributing a policy.

15 Click on the OK button. The PPPoE Option (Create) form closes.

Procedure 54-4 To configure a PPP policy

The 5620 SAM supports PPP configuration on the 7450 ESS, 7750 SR, and 7710 SR.

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Choose PPP Policy (PPP Policy and Session) from the object drop-down list in the Manage Subscriber Policies form.

3 Perform one of the following:

a Create a PPP policy.

i Click on the Create button. A drop down menu appears.

ii Choose PPP Policy. The PPP Policy (Create) form opens.

b Modify a PPP policy.

i Configure the filter criteria and click on the Search button. A list of PPP policies is displayed.

ii Select a PPP policy and click on the Properties button. The PPP Policy (Edit) form opens.

4 Configure the parameters:

- Displayed Name
- Description
- Authentication Type
- Minimum CHAP Challenge Length
- Maximum CHAP Challenge Length
- Disable AC Cookies
- Enable Reply On PADT
- Initial Delay (10s of milliseconds)
- IPCP Subnet Negotiation
- Session Timeout (seconds)
- LCP Keep-Alive Hold Up Multiplier
- LCP Keep-Alive Interval (seconds)
- LCP Ignore Magic Number
- Maximum Sessions Per MAC
- Allow Same Circuit ID For DHCP
- PADO AC Name
- PADO Delay (100s of milliseconds)
- PPP MTU (octets)
- PPP MTU Force Greater Than 1492
- Reject Disabled NCP
- Unique Session ID



Note — Do not use a colon in the policy name; the 5620 SAM uses colons as separators in the object full name.

5 Click on the Apply button. The PPP Policy (Edit) form refreshes.

6 To distribute the policy to an NE, if a local definition does not exist, click on the Local Definitions tab. A list of NEs appears. See Procedure 42-1 for more information about distributing a policy.

7 Click on the Options tab. A list of options is displayed.

8 Perform one of the following:

a To add an option, click on the Create button and go to step 9.

b To edit an existing option, choose an option from the list, click on the Properties button, and go to step 9.

9 In the PPP Option form, configure the parameters:

- Option Protocol
- Custom Option Number
- Option Type
- Option Value
- IP Address

10 Click on the OK button. A dialog box appears.

11 Click on the OK button. The PPP Option (Create) form closes.

12 To configure MLPPP, perform the following steps.

i Click on the MLPPP tab.

ii Configure the parameters.

- Accept MRRU
- Endpoint Type
- Endpoint IPv4 Address
- Endpoint MAC Address
- Receive Short Sequence Number

13 To distribute the policy to an NE, if a local definition does not exist, click on the Local Definitions tab. A list of NEs appears. See Procedure 42-1 for more information about distributing a policy.

14 Click on the OK button. The PPP Policy (Edit) form closes.

Procedure 54-5 To configure an MSAP policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Residential Subscriber form appears.

2 In the Manage Residential Subscriber form, choose Global as the Policy scope and right-click on the Create button to open the contextual menu.

3 Perform one of the following:

a Create a MSAP policy.

i Click on the Create button. A drop down menu appears.

ii Choose Create MSAP Policy. The MSAP Policy - Global (Create) form opens.

b Modify a MSAP Policy.

i Configure the filter criteria and click on the Search button. A list of MSAP policies appears.

ii Select a PPP policy and click on the Properties button. The MSAP Policy (Edit) form opens.

4 Configure the parameters on the General tab:

- Displayed Name
- Description



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

5 Click on the Security tab and configure the parameters.

i In the DoS Protection Policy panel, click on the Select button to open the Select NE DoS Protection Policy form and choose an NE DoS Protection policy.

ii In the DDoS Protection Policy panel, click on the Select button to open the Select NE DDoS Protection Policy form and choose an NE DDoS Protection policy.

iii If MAC Monitoring is required, select the MAC Monitoring check box.

6 Click on the Subscriber Management tab and configure the parameters.

- Subscriber Limit
- Default Subscriber Identification Type
- Default Subscriber ID
- Default Intermediate Destination Id Type
- Default Intermediate Destination Id
- Default Subscriber Profile
- Default SLA Profile
- Default Subscriber Identification Policy
- Default Application Profile
- Profiled Traffic Only
- Non-Subscriber Traffic Identification
- Non-Subscriber Traffic Subscriber Profile
- Non-Subscriber Traffic SLA Profile
- Non-Subscriber Traffic Application Profile

7 Click on the ATM tab.

8 Configure the ATM OAM Alarm Cell Handling and Periodic ATM OAM Loopback parameters.

9 Click on the Select button in the Ingress ATM Policy panel to choose an ingress ATM policy. The Select Ingress ATM Policy - ATM Configuration form opens.

10 Select an ingress ATM policy from the list and click on the OK button. The Select Ingress ATM Policy - ATM Configuration form closes and the MSAP Policy - Global (Create) form refreshes with the ingress ATM policy information displayed.

11 Click on the Select button in the Egress ATM Policy panel to choose an egress ATM policy. The Select Egress ATM Policy - ATM Configuration form opens.

12 Select an egress ATM policy from the list and click on the OK button. The Select Egress ATM Policy - ATM Configuration form closes and the MSAP Policy - Global (Create) form refreshes with the egress ATM policy information displayed.

13 Perform the following as required:

a Click on the VPLS Configuration Only tab and configure the following tabs within the VPLS Configuration Only tab.

i Click on the General tab and configure the parameters:

- Split Horizon Group Name
- Displayed Name
- ARP Reply Agent
- LAG link selection

ii Click on the DHCP tab and configure the parameters:

- Lease Populate
- Action
- Circuit ID
- Remote ID
- Remote ID String
- Vendor Specific Options
- Vendor String
- Administrative State
- Emulated Server IP Address
- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time RADIUS Override

iii Click on the IGMP Snooping tab and configure the parameters:

- IGMP Import Policy
- Fast Leave
- Send Queries
- General Query Interval (seconds)
- Maximum Response Interval (seconds)
- Robust count
- IGMP Version
- Last Member Query Interval (tenths of seconds)
- Name
- Description
- Default Action
- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)
- MVR Source Interface

b If this policy is for an MSAP on an IES or VPRN, click on the IES VPRN Only Configuration tab and configure the Anti-Spoofing parameter to be Source IP and MAC Addr.

c Click on the VPLS Multicast CAC Constraints tab and configure the parameters as follows:



Note 1 — Up to eight Multicast CAC Level entries can be created for an MSAP policy.

Note 2 — Up to eight Multicast CAC LAG entries can be created for an MSAP policy

Note 3 — The Bandwidth (kbps) range is 1 to 4 294 967 952 for an MSAP policy.

i Click on the Create button in the LAG Port Down tab and configure the following parameters:

- Number of Ports Down
- Level ID

ii Click on the Create button in the Level tab and configure the following parameters:

- Level ID
- Bandwidth (kbps)

d Click on the IGMP Host Tracking tab and configure the parameters:

- Expiry Time (seconds)
- Import Policy
- Maximum Number of Groups
- Maximum Number of Sources
- Maximum Number of Group Sources

14 Click on the Apply button.

15 To distribute the policy to an NE, if a local definition does not exist, click on the Local Definitions tab. A list of NEs appears. See Procedure 42-1 for more information about distributing a policy.

16 Click on the OK button.

Procedure 54-6 To configure a host tracking policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Residential Subscriber Policies form opens.

2 Choose Host Tracking Policy (Residential Subscriber) from the object drop-down list in the Manage Residential Subscriber Policies form.

3 Perform one of the following:

a Create a host tracking policy.

i Click on the Create button. A drop down menu appears.

ii Choose Host Tracking Policy. The Host Tracking Policy, Global Policy (Create) form opens.

b Modify a host tracking policy.

i Configure the filter criteria and click on the Search button. A list of host tracking policies appears.

ii Select a host tracking policy and click on the Properties button. The Host Tracking Policy (Edit) form opens.

4 Configure the parameters:

- Displayed Name
- Description
- Rate Modification
- Rate Modification Scheduler



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

5 Click on the Apply button. The Host Tracking Policy (Edit) form refreshes with the policy configuration mode information.

6 To distribute the policy to an NE, if a local definition does not exist, click on the Local Definitions tab. A list of NEs appears. See Procedure 42-1 for more information about distributing a policy.

7 Close the Host Tracking Policy (Edit) form.

Procedure 54-7 To configure a category map policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Residential Subscriber form appears.

2 Click on the Create button to open the contextual menu.

3 Choose Category Map Policy from the contextual menu. The Category Map Policy (Create) form appears with the General tab displayed.

4 Perform one of the following:

a Create a category map policy.

i Click on the Create button. A drop down menu appears.

ii Choose Category Map Policy. The Category Map Policy, Global Policy (Create) form opens.

b Modify a category map policy.

i Configure the filter criteria and click on the Search button. A list of category map policies appears.

ii Select a category map policy and click on the Properties button. The Category Map Policy (Edit) form opens.

5 Configure the parameters:

- Displayed Name
- Description
- Credit Type
- Credit Exhaust Threshold (%)
- Activity Threshold (kbps)

6 Click on the Category tab.

7 Click on the Create button. The Category (Create) form opens with the general tab displayed.

8 Configure the parameters:

- Displayed Name
- Description
- Credit Type Override
- Rating Group
- Out Of Credit Action
- Default Credit Type
- Default Credit Time (seconds)
- Default Credit Volume
- Default Credit Volume Unit
- PIR (kbps)

The Rating Group parameter is only configurable when the Use Rating Group check box is enabled.

The PIR (kbps) parameter is configured to its maximum value when the MAX check box is enabled.



Note — A maximum of three categories can be created for each category map policy.

9 Click on the Queues tab.

10 Select any or all of the Ingress and Egress Queues to be defined in the category.

11 Click on the Policers tab.

12 Select any or all of the Ingress and Egress Policers to be defined in the category.

13 Click on the Credit Exhausting Service Levels tab.

14 Perform one of the following:

a To define credit exhausting service levels for IP filter entries, go to step 15.

b To define credit exhausting service levels for IPv6 filter entries, go to step 21.

15 Click on the IP Filter Entries tab.

16 Click on the Create button. The Exhausted IP Filter Entry (Create) form opens with the General tab displayed.

17 Configure the parameters:

- Filter Direction
- Entry ID
- Displayed Name
- Description

18 Click on the Filter Properties tab.

19 Configure the parameters:

- Action
- Protocol
- DSCP
- Source IP Address
- Src Mask
- Destination IP Address
- Dst Mask
- Fragment
- IP Option
- IP Opt Mask
- Option Present
- Multiple Option

20 Go to step 26.

21 Click on the IPv6 Filter Entries tab.

22 Click on the Create button. The Exhausted IPv6 Filter Entry (Create) form opens.

23 Configure the parameters:

- Filter Direction
- Entry ID
- Displayed Name
- Description

24 Click on the Filter Properties tab.

25 Configure the parameters:

- Action
- Protocol
- DSCP
- Source IP Address
- Src Mask
- Destination IP Address
- Dst Mask

26 Click on the OK button. A dialog box appears.

27 Click on the OK button. The Category (Create) for reappears with the filter entries information displayed.

28 Click on the OK button. A dialog box appears.

29 Click on the OK button. The Category Map Policy (Create) form reappears with the category information displayed.

30 To distribute the policy to an NE, if a local definition does not exist, click on the Local Definitions tab. A list of NEs appears. See Procedure 42-1 for more information about distributing a policy.

31 Click on the OK button. The Category Map Policy (Create) form closes.

Procedure 54-8 To configure a credit control policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Residential Subscriber form appears.

2 Click on the Create button to open the contextual menu.

3 Choose Credit Control Policy from the contextual menu. The Credit Control Policy (Create) form opens with the General tab displayed.

4 Perform one of the following:

a Create a credit control policy.

i Click on the Create button. A drop down menu appears.

ii Choose Category Map Policy. The Credit Control Policy (Create) form opens.

b Modify a credit control policy.

i Configure the filter criteria and click on the Search button. A list of credit control policies appears.

ii Select a category map policy and click on the Properties button. The Credit Control Policy (Edit) form opens.

5 Configure the parameters:

- Displayed Name
- Description
- Credit Control Server
- Out Of Credit Action
- Error Handling Action

6 Click on the Select button in the Category Map panel. The Select Category Map form opens.

7 Select a category map policy from the list to be used with the credit control policy and click on the OK button. The Select Category Map form closes.

8 If you selected a value of Diameter for the Credit Control Server parameter, click on the Select button in the Diameter Policy panel. The Select Diameter Policy form opens.

9 Select a diameter policy from the list to be used to access the credit control server and click on the OK button. The Select Diameter Policy panel closes.

10 To distribute the policy to an NE, if a local definition does not exist, click on the Local Definitions tab. A list of NEs appears. See Procedure 42-1 for more information about distributing a policy.

11 Click on the OK button. The Credit Control Policy (Create) form closes.

Procedure 54-9 To configure an IGMP policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Residential Subscriber Policies form opens.

2 Choose IGMP Policy (Residential Subscriber) from the object drop-down list in the Manage Residential Subscriber Policies form.

3 Perform one of the following:

a Create an IGMP policy.

i Click on the Create button. A drop down menu appears.

ii Choose Create IGMP Policy. The IGMP Policy, Global Policy (Create) form opens.

iii Go to step 4.

b Modify an IGMP policy.

i Configure the filter criteria and click on the Search button. A list of IGMP policies appears.

ii Select an IGMP policy and click on the Properties button. The IGMP Policy (Edit) form opens.

4 Configure the parameters:

- Displayed Name
- Description
- Import Policy
- Maximum Number Of Groups
- Maximum Number Of Sources
- Maximum Number Of Group Sources
- Administrative Version
- Fast Leave
- Redirection Policy



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

5 Configure the parameters in the multicast reporting panel:

- Administrative State
- Destination Name
- SAP ID
- Service ID
- PPPoE Session ID
- Host MAC

6 Click on the Apply button. The IGMP Policy (Edit) form refreshes with the policy configuration mode information.

7 Click on the Static Group/Source tab. A list of multicast static group/static source address pairs appears.

8 Perform one of the following:

a Select an address pair from the list and click on the Properties button. The IGMP Policy Static (Edit) form appears. Go to step 9.

b Click on the Create button. The IGMP Policy Static (Create) form appears. Go to step 9.

9 Configure the parameters:

- Static Multicast Group
- Static Source

10 To distribute the policy to an NE, if a local definition does not exist, click on the Local Definitions tab. A list of NEs appears. See Procedure 42-1 for more information about distributing a policy.

11 Close the IGMP Policy (Edit) form.

Procedure 54-10 To configure a BGP Peering policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Residential Subscriber Policies form opens.

2 Choose BGP Peering Policy (Residential Subscriber) from the object drop-down list in the Manage Residential Subscriber Policies form.

3 Perform one of the following:

a Create a BGP Peering policy.

i Click on the Create button. A drop down menu appears.

ii Choose Create BGP Peering Policy. The BGP Peering Policy, Global Policy (Create) form opens.

iii Go to step 4.

b Modify a BGP Peering policy.

i Configure the filter criteria and click on the Search button. A list of BGP Peering policies appears.

ii Select a BGP Peering policy and click on the Properties button. The BGP Peering Policy (Edit) form opens.

4 Configure the parameters:

If the Inherit Value box is enabled for a parameter, the parameter value is inherited from the parent BGP object.

- Displayed Name
- Description
- Cluster ID
- Local Address
- BGP Keychain
- MED Source
- MED Value



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

5 Click on the Apply button. The BGP Peering Policy (Edit) form refreshes with the policy configuration mode information.

6 Click on the Behavior tab and configure the parameters:

If the Inherit Value box is enabled for a parameter, the parameter value is inherited from the parent BGP object.

- Preference
- Local Preference
- Multi Hop
- Loop Detect
- Aggregator ID Zero
- Damping
- Disable Client Reflect
- Min. Route Advertisement
- Disable Standard Communities
- Disable Extended Communities
- Disable Fast External Failover
- Advertise Inactive Routes
- Peer Type
- Passive
- Next Hop Self
- Minimum TTL Value
- Connect Retry Time (seconds)
- Keep Alive (seconds)
- Hold Time (seconds)
- Prefix Limit

7 Click on the AS Properties tab and configure the parameters:

If the Inherit Value box is enabled for a parameter, the parameter value is inherited from the parent BGP object.

- Peer AS
- Min AS Origination (seconds)
- Disable 4Byte ASN
- AS Override
- Local AS
- Remove Private AS

8 Click on the Import Policies tab and configure the parameters:

If the Inherit Value box is enabled for a parameter, the parameter value is inherited from the parent BGP object.

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

9 Click on the Export Policies tab and configure the parameters:

If the Inherit Value box is enabled for a parameter, the parameter value is inherited from the parent BGP object.

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

10 Click on the Authentication tab and configure the parameters:

If the Inherit Value box is enabled for a parameter, the parameter value is inherited from the parent BGP object.

- MD5 Authentication
- Authentication Key

11 To distribute the policy to an NE, if a local definition does not exist, click on the Local Definitions tab. A list of NEs appears. See Procedure 42-1 for more information about distributing a policy.

12 Close the BGP Peering Policy (Edit) form.

Procedure 54-11 To configure a diameter policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Residential Subscriber Policies form opens.

2 Perform one of the following.

a Create a diameter policy.

i Click on the Create button and choose Diameter Policy from the drop-down menu. The Diameter Policy (Create) form appears with the General tab displayed.

ii Go to step 3.

b Modify a diameter policy.



Caution — Modifying an active diameter policy is potentially service-affecting. Ensure that you consider the implications of reconfiguring the diameter policy before you proceed.

i Choose Diameter Policy from the object drop-down list.

ii Configure the filter criteria and click on the Search button. A list of diameter policies appears.

iii Select a diameter policy and click on the Properties button. The Diameter Policy (Edit) form opens.

3 Configure the parameters:

- Displayed Name
- Description

4 On the Connection Origin panel, configure the Virtual Router Type parameter.

If you specified VPRN Service as the Virtual Router Type, you must also configure the Service Name parameter on the VPRN Service panel. Click on the Select button and choose a VPRN service from the Select VPRN Service - Diameter Policy form.

5 Configure the timer parameters:

- Watchdog Timer (seconds)
- Connection Timer (seconds)
- Transaction Timer (seconds)

6 On the Vendor support panel, configure the Vendor parameter.

7 Click on the DCAA Parameters tab.

8 Configure the parameters:

- Failover Support
- Failure Handling
- Tx Timer (seconds)
- Service Context ID
- RADIUS Called-Station-ID
- Include RADIUS User
- Origin Subscription ID
- Subscription ID Type
- Origin 3GPP IMSI

9 Click on the Peers tab.

10 Click on the Create button. The Diameter Peer - Diameter Policy (Create) form appears with the General tab displayed.

11 Configure the parameters:

- Displayed Name
- Description
- Administrative State
- Preference
- IP Address
- Port Number
- Protocol
- Destination Host
- Destination Realm

12 If you want to specify local override settings for any of the timer settings for the peer, deselect the Inherit Value check box and then specify a value for any of the following timer parameters:

- Watchdog Timer (seconds)
- Connection Timer (seconds)
- Transaction Timer (seconds)



Note — When the Inherit Value check box is selected for a timer parameter on a peer object, the timer value is inherited from the parent diameter policy.

13 Click on the OK button on Diameter Peer - Diameter Policy (Create) form. The Diameter Policy (Create) form reappears with the new peer displayed on the Peers tab.

14 To distribute the policy to an NE, if a local definition does not exist, click on the Local Definitions tab. A list of NEs appears. See Procedure 42-1 for more information about distributing a policy.

15 Click on the OK button in the Diameter Policy (Create) form. The Manage Residential Subscriber Policies form reappears with the new diameter policy displayed in the list.

Procedure 54-12 To configure a subscriber multicast CAC policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Perform one of the following.

a Create a subscriber multicast CAC policy.

i Click on the Create button and choose Create Subscriber Multicast CAC Policy from the drop-down menu. The Subscriber Multicast CAC Policy (Create) form opens.

ii Go to step 3.

b Modify a subscriber multicast CAC policy.

i Choose Subscriber Multicast CAC Policy from the object drop-down list.

ii Configure the filter criteria and click on the Search button. A list of subscriber multicast CAC policies appears.

iii Select a subscriber multicast CAC policy and click on the Properties button. The Subscriber Multicast CAC Policy (Edit) form opens.

3 Configure any applicable parameters:

- Displayed Name
- Description
- Administrative State
- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 To distribute the policy to an NE, if a local definition does not exist, click on the Local Definitions tab. A list of NEs appears. See Procedure 42-1 for more information about distributing a policy.

5 Click on the OK button. The Subscriber Multicast CAC Policy (Create) form closes.

Procedure 54-13 To configure a mobile gateway profile

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Perform one of the following.

a Create a mobile gateway profile.

i Click on the Create button and choose Mobile Gateway Profile from the drop-down menu. The Mobile Gateway Profile form opens.

ii Go to step 3.

b Modify a mobile gateway profile.

i Choose Mobile Gateway Profile from the object drop-down list.

ii Configure the filter criteria and click on the Search button. A list of mobile gateway profiles appears.

iii Select a mobile gateway profile and click on the Properties button. The Mobile Gateway Profile (Edit) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- IP TTL
- Interface Type



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 If you want to specify non-default message-retransmit parameters, disable the Message-Retransmit - Default parameter and configure the Message-Retransmit - Timeout (seconds) and Message-Retransmit - Retries parameters.

5 If you want to specify non-default keep-alive parameters, disable the Keep-Alive - Default parameter and configure the Keep-Alive - Interval (seconds), Keep-Alive - Timeout (seconds), and Keep-Alive - Retries parameters.

6 On the Charging Characteristics panel, configure home charging characteristics and roaming charging characteristics, as required.

7 Configure packet data network gateway QoS parameters, as required.

i Click on the PGW tab.

ii Disable the Default parameter to configure the Allocation/Retention Priority (ARP) parameter.

iii Disable the Default parameter on the Downlink panel to configure the GBR and MBR parameters.

iv Disable the Default parameter to configure the Class Identifier (QCI) parameter.

v Disable the Default parameter on the Uplink panel to configure the GBR and MBR parameters.

8 Configure gateway GPRS support node QoS parameters, as required.

i Click on the GGSN tab.

ii Disable the Default parameter to configure the Allocation/Retention Priority (ARP) parameter.

iii Disable the Default parameter on the Downlink panel to configure the GBR and MBR parameters.

iv Disable the Default parameter on the Uplink panel to configure the GBR and MBR parameters.

9 To distribute the policy to an NE, if a local definition does not exist, click on the Local Definitions tab. A list of NEs appears. See Procedure 42-1 for more information about distributing a policy.

10 Click on the OK button. The Mobile Gateway Profile form closes.

Procedure 54-14 To configure a host lockout policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Perform one of the following.

a Create a host lockout policy.

i Click on the Create button and choose Host Lockout Policy from the drop-down menu. The Host Lockout Policy form opens.

ii Go to step 3.

b Modify a host lockout policy.

i Choose Host Lockout Policy from the object drop-down list.

ii Configure the filter criteria and click on the Search button. A list of host lockout policies appears.

iii Select a host lockout policy and click on the Properties button. The Host Lockout Policy (Edit) form opens.

3 Configure any applicable parameters:

- Displayed Name
- Description
- Minimum Lockout Time
- Maximum Lockout Time
- Reset Time
- Maximum Lockout Hosts (per SAP)



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 To distribute the policy to an NE, if a local definition does not exist, click on the Local Definitions tab. A list of NEs appears. See Procedure 42-1 for more information about distributing a policy.

5 Click on the OK button. The Host Lockout Policy form closes.

Procedure 54-15 To clear host lockouts

Perform this procedure to clear host lockouts enforced by a specific host lockout policy. Lockouts can be cleared at the policy level, or they can be cleared from a NE with which the policy is associated. Host lockouts can also be cleared from IES or VPRN SAPs.

1 To clear host lockouts, do one of the following:

a To clear host lockouts at the host lockout policy level or NE level, complete steps 2 through 14.

b To clear host lockouts from a SAP on an IES or VPRN, complete steps 15 through 14.

2 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

3 Choose Host Lockout Policy from the object drop-down list.

4 Configure the filter criteria and click on the Search button. A list of host lockout policies appears.

5 Select the host lockout policy for which you want to clear lockouts and click on the Properties button. The Host Lockout Policy form opens.

6 Click on the Local Definitions tab.

7 Click on the Search button. A list of policy definitions appears.

8 Select a policy definition in the list and click on the Properties button.

9 In the Policy Definition Properties form, click on the Clear Host Lockout Policy button.

10 Choose one of the following options:

- Network Element: all host lockouts are cleared from the associated NE.
- Policy: all host lockouts are cleared for the selected policy.

11 Click on the OK button. The lockouts are cleared.

12 Click on the OK button. The Policy Definition Properties form closes.

13 Click on the OK button. The Host Lockout Policy form closes.

14 Close the Manage Subscriber Policies form.

15 To clear host lockouts from IES or VPRN service SAPs, choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

16 Configure the search criteria and click on the Search button. A list of services appears.

17 Choose a service that has SAPs from which you want to clear host lockouts, and then click on the Properties button. The service properties form appears.

18 On the navigation tree, expand the Subscriber Interfaces object, and then expand a group interface object to navigate to the SAP from which you want to clear host lockouts.

19 Right-click on the SAP object and choose Properties from the menu. The Service Access Point form appears.

20 Click on the Subscriber Management tab, and then click on the Locked Out Hosts tab.

21 Click on the Search button to display a list of locked out hosts.

22 Click on the Clear Locked Out Hosts button. You can either clear all host lockouts on the SAP, or you can clear lockout selectively by specifying ID criteria.

23 Click on the OK button. The lockouts are cleared.

24 Click on the OK button. The Service Access Point form closes.

25 Click on the OK button. The service properties form closes.

26 Close the Manage Services form.

Procedure 54-16 To configure a RADIUS script policy

Perform this procedure to create a RADIUS script policy. A RADIUS script policy references python scripts for RADIUS AAA packet manipulation in a subscriber management application.

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Perform one of the following.

a Create a RADIUS script policy.

i Click on the Create button and choose RADIUS Script Policy from the drop-down menu. The RADIUS Script Policy form opens.

ii Go to step 3.

b Modify a RADIUS script policy.

i Choose RADIUS Script Policy from the object drop-down list.

ii Configure the filter criteria and click on the Search button. A list of RADIUS script policies appears.

iii Select a RADIUS script policy and click on the Properties button. The RADIUS Script Policy (Edit) form opens.

3 Configure any applicable parameters:

- Displayed Name
- Description
- Action on fail
- Primary Script URL
- Primary Script Admin State
- Secondary Script URL
- Secondary Script Admin State

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 To distribute the policy to an NE, if a local definition does not exist, click on the Local Definitions tab. A list of NEs appears. See Procedure 42-1 for more information about distributing a policy.

5 Click on the OK button. The RADIUS Script Policy form closes.

6 Close the Residential Subscriber Policies form.

Procedure 54-17 To configure an SLA profile

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Perform one of the following.

a Create an SLA profile.

i Click on the Create button and choose Create SLA Profile from the drop-down menu. The SLA Profile (Create) form opens.

ii Go to step 3.

b Modify an SLA profile.



Caution — Modifying an active SLA profile is potentially service-affecting. Ensure that you consider the implications of reconfiguring the SLA profile before you proceed.

i Choose SLA Profile from the object drop-down list.

ii Configure the filter criteria and click on the Search button. A list of SLA profiles appears.

iii Select an SLA profile and click on the Properties button. The SLA Profile (Edit) form opens.

3 Configure the parameters:

- Displayed Name
- Application
- Description
- Host Limit
- Remove oldest Subscriber Host

The Displayed Name parameter is configurable only during SLA profile creation.



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Select button in the Credit Control Policy panel. The Select Credit Control Policy form opens.

5 Select a credit control policy from the list and click on the OK button. The Select Credit Control Policy form closes.



Note — If you select a credit control policy, you will not be able to select a category map in step 13.

6 Click on the QoS tab to choose QoS policies for the SLA profile.

7 Perform one of the following steps using the buttons in the Ingress Policy and Egress Policy panels.

a Assign a policy.

i Click on the appropriate Select button to choose an ingress or egress QoS policy. The ingress or egress Select Policy - SLA Profile form opens.

ii Select a policy and click on the OK button. The Select Policy - SLA Profile form closes, and the SLA Profile (Create) form refreshes with the chosen policy.

iii Configure the ingress queue parameters:

- Use Shared Queue
- Use Multipoint Shared Queue
- Report Rate Type
- Report Rate Scheduler

iv Configure the egress QoS marking parameters:

- Use Egress QoS Marking From SAP
- Scheduler Type
- Report Rate Type
- Report Rate Scheduler
- Use Ingress L2TP DSCP

b Remove a policy.

i Click on the Clear button in the Ingress Policy or Egress Policy panel to remove an ingress or egress QoS policy. The policy is removed from the list.

ii If you want to assign a policy to replace the removed policy, go to step 7a.

8 Click on the ACL tab to assign ingress or egress IP filters to the SLA profile, if required.

i Click on the Select button in the Ingress IP Filter panel to choose an ingress IP filter from the Select Ingress IP Filter - SLA Profile form.

ii Click on the Select button in the Egress IP Filter panel to choose an egress IP filter from the Select Egress IP Filter - SLA Profile form.

iii Click on the Select button in the Ingress IPv6 Filter panel to choose an ingress IPv6 filter from the Select Ingress IPv6 Filter - SLA Profile form.

iv Click on the Select button in the IPv6 Egress Filter panel to choose an IPv6 egress filter from the Select Egress IPv6 Filter - SLA Profile form.

v Click on the Select button in the One-Time HTTP Redirect Filter panel to choose an ACL IP filter with an HTTP redirect from the Select One-Time HTTP Redirect Filter form.

9 Click on the Supported Service Models tab to indicate the intended service model for the SLA profile.



Note — The 5750 SSC requires the specification of a service model for interoperation with the 5620 SAM.

10 Configure the parameters:

- VLAN per Subscriber (Routed)
- VLAN per Service (Routed)
- VLAN for all Services (Routed)
- VLAN per ISP per Service (Routed)
- VLAN per Subscriber (Bridged)
- VLAN per Service (Bridged)
- VLAN for all Services (Routed)
- VLAN per ISP per Service (Bridged)

11 Click on the Category Map tab.

12 Click on the Select button in the Category Map panel. The Select Category Map form opens.

13 Select a category map from the list and click on the OK button. The Select Category Map form closes.



Note — If you selected a credit control policy in step 5, you will not be able to select a category map.

14 Click on the Create... button in the Categories panel. The Category (Create) form opens.

15 Click on the Select button in the Category Name panel. The Select Category Name form opens.

16 Select a category name from the list and click on the OK button. The Select Category Name form closes and the Category (Create) form reappears with the category name displayed.

17 Configure the Idle Timeout (seconds) parameter.



Note — The session will be disconnected if the value of the Activity Threshold (kbps) parameter is not met during the period specified by the Idle Timeout (seconds) parameter. See procedure 54-7 for more information about configuring the Activity Threshold (kbps) parameter.

18 Click on the OK button. A dialog box appears.

19 Click on the OK button.

20 Click on the Override Policy Items tab to specify local overrides for queue parameters of the QoS policies assigned to the SLA profile, if required. The Access Ingress Policy tab is displayed.

21 Perform either of the following:

a Modify the access ingress queue parameters.

i Click on the Create button. The Access Ingress Queue Override (Create) form opens with the General tab displayed.

ii Go to step 22.

b Modify the access egress queue parameters.

i Click on the Access Egress Queues tab.

ii Click on the Create button. The Access Egress Queue Override (Create) form opens with the General tab displayed.

22 Choose the policy queue that you want to override.

i Click on the Select button. The policy queue Select form opens.

ii Select a policy queue and click on the OK button. The policy queue Select form closes, and the Queue Override (Create) form refreshes with the configured values for the policy queue.

23 Click on the Override tab and configure the parameters:

• Override PIR	• CIR (kbps)
• Override CIR	• CIR (kbps)
• Override Maximum Burst Size	• Maximum Burst Size (bytes)
• Override Committed Burst Size	• Committed Burst Size (kb)
• Override High Priority Reserved	• High Priority Reserved
• Override Port Average Overhead	• Port Average Overhead (%)
• Default	

The Override Port Average Overhead and Port Average Overhead (%) parameters are configured only for access egress queues.

24 Click on the OK button to close the Queue Override (Create) form. A dialog box appears.

25 Click on the OK button. The SLA Profile (Create) form refreshes with the queue override entry.

26 Specify local overrides for statistics and traffic flow rate parameters of the ingress or egress policers assigned to the SLA profile, if required.

27 Perform either of the following:

a Modify the access ingress policer parameters.

i Click on the Access Ingress Policers tab.

ii Click on the Create button. The Ingress Policer Override (Create) form opens with the General tab displayed.

iii Go to step 28.

b Modify the access egress policer parameters.

i Click on the Access Egress Policer tab.

ii Click on the Create button. The Egress Policer Override (Create) form opens with the General tab displayed.

28 Choose the policy policer that you want to override.

i Click on the Select button. The policy policer Select form opens.

ii Select a policy policer and click on the OK button. The policy policer Select form closes, and the Policer Override (Create) form refreshes with the configured values for the policy policer.

29 Click on the Override tab and configure the parameters:

- Override PIR
- Override CIR
- Override Maximum Burst Size
- Override Committed Burst Size
- Default
- CIR (kbps)
- CIR (kbps)
- Maximum Burst Size (bytes)
- Committed Burst Size (kb)
- Stats Mode
- Packet Byte Offset

30 Click on the OK button to close the Policer Override (Create) form. A dialog box appears.

31 Click on the OK button. The SLA Profile (Create) form refreshes with the policy policer override entry.

32 Click on the OK button. A dialog box appears.

33 To distribute the policy to an NE, if a local definition does not exist, click on the Local Definitions tab. A list of NEs appears. See Procedure 42-1 for more information about distributing a policy.

34 Click on the Yes button. The SLA Profile (Create) form closes.

Procedure 54-18 To configure a subscriber profile

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Perform one of the following.

a Create a subscriber profile.

i Click on the Create button and choose Create Subscriber Profile from the drop-down menu. The Subscriber Profile (Create) form opens.

ii Go to step 3.

b Modify a subscriber profile.



Caution — Modifying an active subscriber profile is potentially service-affecting. Ensure that you consider the implications of reconfiguring the subscriber profile before you proceed.

i Choose Subscriber Profile from the object drop-down list.

ii Configure the filter criteria and click on the Search button. A list of subscriber profiles appears.

iii Select a subscriber profile and click on the Properties button. The Subscriber Profile (Edit) form opens.

3 Configure the parameters:

- Displayed Name
- Description
- Preference



Note 1 — You can designate a subscriber profile as the default profile by specifying the case-sensitive name “default” for the Displayed Name parameter. The Displayed Name parameter is configurable only during subscriber profile creation.

Note 2 — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

Note 3 — The Egress Aggregate Rate Limit (kbps) and Frame Base Accounting parameters are configurable only when a scheduler is not specified in the Egress Scheduler panel.

4 Click on the Select button in the Accounting Policy panel and choose an accounting policy from the Select Accounting Policy ID - Subscriber Profile form.

5 Click on the Select button in the ANCP Policy panel and choose an ANCP policy from the Select ANCP Policy - Subscriber Profile form.

6 Click on the Select button in the Host Tracking Policy panel and choose a host tracking policyfrom the Select Host Tracking Policy - Subscriber Profile form.

7 Click on the Select button in the NAT Policy panel and choose a NAT policy from the Select NAT Policy - Subscriber Profile form.

8 Click on the Select button in the IGMP Policy panel and choose an IGMP policy from the Select IGMP Policy - Subscriber Profile form.

9 Click on the Select button in the Subscriber Multicast CAC Policy panel and choose a subscriber multicast CAC policy from the Select Subscriber Multicast CAC Policy - Subscriber Profile form.

10 Click on the Scheduling tab.

11 Configure the parameters:

- Assign Aggregate Rate Limit
- Egress Aggregate Rate Limit (kbps)
- Average Frame Size
- Encap Offset
- Frame Base Accounting



Note — An additional parameter, Encapsulation Offset Mode, can be configured using OSSI.

12 Assign an ingress or egress scheduler. Click on the appropriate Select button to choose an ingress or egress scheduler from the ingress or egress Select Scheduler - Subscriber Profile form.



Note — You cannot specify an egress scheduler in a subscriber profile when the Egress Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

13 Click on the RADIUS Accounting tab.

i Click on the Select button in the RADIUS Accounting Information panel and choose a policy from the Select RADIUS Accounting Information - Subscriber Profile form.

ii Click on the Select button in the Duplicate RADIUS Accounting Information panel and choose a policy from the Select Duplicate RADIUS Accounting Information - Subscriber Profile form.

14 Click on the SLA Profiles tab. The General tab is displayed.

15 Configure the Use Direct Map as Default parameter.

16 Click on the Profiles tab.

i Click on the Create button. The SLAProfileEntry form opens.

ii Click on the Select button to choose an SLA profile. The Select SLA Profile form opens.

iii Select an SLA profile and click on the OK button. The Select SLA Profile form closes, and the SLAProfileEntry form refreshes with the SLA profile information.

iv Configure the SLA Profile String parameter.

v Click on the OK button to close the SLAProfileEntry form. A dialog box appears.

vi Click on the OK button. The Subscriber Profile form refreshes with the SLA profile entry.

vii Repeat steps i through vi for each additional SLA profile that you want to associate with the subscriber profile.

17 Click on the HSMDA QoS tab.

18 Perform one of the following.

a Assign an ingress policy. Click on the Select button in the Ingress Policy panel and choose an ingress policy from the Select Ingress Policy form.

b Assign an egress policy.

i Configure the Aggregate Rate Limit parameter

ii Click on the Select button in the Egress Policy panel and choose an egress policy from the Select Egress Policy form.

19 Configure the Packet Byte Offset (bytes) parameter in the Egress Policy Override panel, if required. You must enable the associated Override check box to be able to configure this parameter.

20 Click on the Select button in the Egress Policy Override panel and choose a WRR policy from the Select WRR Policy form.

21 Click on the Policer Control tab to configure ingress and egress policer control policies, if required:

i On the Ingress Policer Control Policy panel, click on the Select button beside the Displayed Name field and choose a policy from the Select Policer Control Policy form.

ii You can configure local overrides on the selected ingress policer control policy on the Ingress Policer Control Policy Override panel, if required. Enable the Override check box for either of the following parameters, and then configure the parameters:

- Maximum Frame Based Bandwidth
- Minimum Separation Buffer Space

iii On the Egress Policer Control Policy panel, click on the Select button beside the Displayed Name field and choose a policy from the Select Policer Control Policy form.

iv You can configure local overrides on the selected egress policer control policy on the Egress Policer Control Policy Override panel, if required. Enable the Override check box for either of the following parameters, and then configure the parameters:

- Maximum Frame Based Bandwidth
- Minimum Separation Buffer Space

22 Click on the Override Policy Items tab to modify the scheduler parameters for the subscriber profile, if required.

23 Perform one of the following.

a Modify the ingress scheduler parameters.

i Click on the Ingress Schedulers tab.

ii Click on the Create button. The Ingress Scheduler Entry Override form opens with the General tab displayed.

iii Click on the Select button and choose a scheduler policy from the Select Ingress Scheduler Policy Entry form.

iv Click on the Override tab.

v Configure the parameters:

- Summed CIR
- PIR (kbps)
- CIR (kbps)

The CIR (kbps) parameter can only be configured when Summed CIR is set to false.

vi Click on the OK button to close the Ingress Scheduler Entry Override form.

b Modify the egress scheduler parameters.

i Click on the Egress Schedulers tab.

ii Click on the Create button. The Egress Scheduler Entry Override form opens with the General tab displayed.

iii Click on the Select button and choose a policy from the Select Egress Scheduler Policy Entry form.

iv Click on the Override tab.

v Configure the parameters:

- Summed CIR
- PIR (kbps)
- CIR (kbps)

The CIR (kbps) parameter can only be configured when Summed CIR is set to false.

vi Click on the OK button to close the Egress Scheduler Entry Override form.

c Modify the access egress HSMDA queue parameters.

i Click on the Access Egress HSMDA Queues tab.

ii Click on the Create button. The Access Egress HSMDA Queue Override form opens with the General tab displayed.

iii Click on the Select button and choose a queue from the Select Access Egress Policy Queue form.

iv Click on the Override tab.

v Configure the parameters:

- PIR (kbps)
- Maximum Burst Size (bytes)
- WRR Weight

If you enable the Override check box for any of these parameters, then the original value of the parameter that was configured for the Access Egress HSMDA Queue will appear in that parameter's value field. You can then configure the override value for that parameter.

You can only specify an override value for WRR Weight for queues 1, 2, or 3.

vi Click on the Select button and choose a policy from the Select HSMDA Slope Policy form.

vii Click on the OK button to close the Access Egress HSMDA Queue Override form.

d Click on the Ingress Policer Level tab to configure ingress policer priority level overrides, if required. An ingress policer control policy must be configured on the subscriber profile before these steps can be completed.

i Click on the Create button. The Ingress Policer Level Override form appears. The configured policer control policy appears in the Displayed Name field.

ii On the Policer Level panel, click on the Select button and choose a policer level from the Select Policer Level form.

The current maximum cumulative buffer space value for the policer level is displayed in the Maximum Cumulative Buffer Space field.

iii To override the maximum cumulative buffer space value for the policer level, click on the Override tab.

iv On the Overridden Policer Level panel, enable the Override check box.

v Either enable the Max check box or configure the Cumulative MBS Contribution parameter.

vi Click OK. The policer level override is applied to the subscriber profile. To configure additional policer level overrides, repeat steps i through vi.

e Click on the Egress Policer Level tab to configure egress policer priority level overrides, if required. An egress policer control policy must be configured on the subscriber profile before these steps can be completed.

i Click on the Create button. The Egress Policer Level Override form appears. The configured policer control policy appears in the Displayed Name field.

ii On the Policer Level panel, click on the Select button and choose a policer level from the Select Policer Level form.

The current maximum cumulative buffer space value for the policer level is displayed in the Maximum Cumulative Buffer Space field.

iii To override the maximum cumulative buffer space value for the policer level, click on the Override tab.

iv On the Overridden Policer Level panel, enable the Override check box.

v Either enable the Max check box or configure the Cumulative MBS Contribution parameter.

vi Click OK. The policer level override is applied to the subscriber profile. To configure additional policer level overrides, repeat steps i through vi.

24 Click on the OK button. The Subscriber Profile form refreshes with the scheduler override entry.

25 Click on the OK button to close the Subscriber Profile form. A dialog box appears.

26 To distribute the policy to an NE, if a local definition does not exist, click on the Local Definitions tab. A list of NEs appears. See Procedure 42-1 for more information about distributing a policy.

27 Click on the Yes button. The Subscriber Profile form closes.

Procedure 54-19 To configure a subscriber explicit map

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Perform one of the following.

a Create a subscriber explicit map entry.

i Click on the Create button and choose Create Subscriber Explicit Map Entry from the drop-down menu. The Subscriber Explicit Map Entry (Create) form opens.

ii Go to step 3.

b Modify a subscriber explicit map entry.



Caution — Modifying an active subscriber explicit map entry is potentially service-affecting. Ensure that you consider the implications of reconfiguring the subscriber explicit map entry before you proceed.

i Choose Subscriber Explicit Map Entry from the object drop-down list.

ii Configure the filter criteria and click on the Search button. A list of subscriber explicit map entries appears.

iii Select a subscriber explicit map entry and click on the Properties button. The Subscriber Explicit Map Entry (Edit) form opens.

3 Configure the parameters:

- Subscriber Identification
- Description
- Subscriber ID Alias

The Subscriber Identification parameter is configurable only during subscriber explicit map creation.

4 Click on the Select button in the Subscriber Profile panel to associate a subscriber profile with the subscriber explicit map. The Select Subscriber Profile form opens.

5 Select a subscriber profile and click on the OK button. The Select Subscriber Profile form closes, and the Subscriber Explicit Map Entry (Create) form refreshes with the subscriber profile.

6 Click on the Select button in the SLA Profile panel to associate an SLA profile with the subscriber explicit map. The Select SLA Profile form opens.

7 Select an SLA profile and click on the OK button. The Select SLA Profile form closes and the Subscriber Explicit Map Entry (Create) form refreshes with the SLA profile.

8 Click on the Select button in the Application Profile panel to associate an application profile with the subscriber explicit map. The Select Application Profile form opens.

9 Select an application profile and click on the OK button. The Select Application Profile form closes and the Subscriber Explicit Map Entry (Create) form refreshes with the application profile.



Note 1 — The global AA group policy must be manually distributed to the NE before a global subscriber identification policy using the application profiles can be distributed.

Note 2 — When a new subscriber identification or subscriber explicit map is discovered from the NE, the AA group policy is not automatically resynchronized to the global subscriber identification policy.

10 Click on the OK button to close the Subscriber Explicit Map Entry (Create) form.

55 — Remote network monitoring policies

55.1 Remote network monitoring policies overview *55-2*

55.2 Remote network monitoring policies procedures *55-2*

55.1 Remote network monitoring policies overview

You can create remote network monitoring (RMON) policies that allow you to perform the following tasks.

- Use the policy framework to configure RMON that allows 5620 SAM users to deploy configurations to multiple devices.
- Map RMON events to information alarms in the 5620 SAM GUI.

Remote network monitoring allows you to monitor the behavior of functions that are not typically supported by the 5620 SAM. For example, you can configure events on GNEs to monitor system temperature or CPU usage. The 5620 SAM can raise informational alarms for the exceeded thresholds. You can also configure custom values to supersede the hard-coded threshold values associated with an NE function.

The 5620 SAM maps RMON SNMP traps to alarms in the GUI.

Policy distribution and event mapping are supported for the following NE types:

- 7210 SAS-M
- 7210 SAS-T
- 7210 SAS-X
- 7450 ESS
- 7710 SR
- 7750 SR
- 7950 XRS

55.2 Remote network monitoring policies procedures

The following procedures describe how to configure and manage RMON policies.

Procedure 55-1 To configure a remote network monitoring policy

1 Choose Tools→Remote Network Monitoring (RMON) from the 5620 SAM main menu. The Remote Network Monitoring (RMON) form opens.

2 Perform one of the following:

  a Specify a filter to search for an existing policy. Select a policy in the filtered list and click on the Properties button.

  b Click on the Create button. The RMON (Create) form opens.

3 Configure the parameters:

- Displayed Name
- Description



Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Create events to associate with the rising and falling thresholds on the remote NE.

i Click on the Events tab.

ii Click on the Create button. The Event RMON (Create) form opens.

iii Configure the parameters:

- Auto-Assign ID
- ID
- Displayed Name
- Description
- Type
- Owner
- Community

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Event RMON (Create) form closes and the RMON (Create) form reappears.

vi Repeat steps 4ii to v to create another event, if required.

5 Configure the alarm information that is associated with the remote event.

i Click on the Alarms tab.

ii Click on the Create button. The Alarm RMON form opens.

iii Configure the parameters:

- Auto-Assign ID
- ID
- Displayed Name
- Description
- Monitored Object OID
- Interval (seconds)
- Sample Type
- Start Up Alarm
- Owner

6 Configure the properties for the rising threshold crossing alarm.

i Click on the Select button in the Rising TCA Properties panel. The Select Rising Event - Alarm form opens.

ii Select the event and click on the OK button. The Select Rising Event - Alarm form closes and the Alarm RMON form reappears.

iii Configure the Rising Threshold parameter.

7 Configure the properties for the falling threshold crossing alarm.

i Click on the Select button in the Falling TCA Properties panel. The Select Falling Event - Alarm form opens.

ii Select the event and click on the OK button. The Select Falling Event - Alarm form closes and the Alarm RMON form reappears.

iii Configure the Falling Threshold parameter.

8 Click on the OK button. A dialog box appears.

9 Click on the OK button. The Alarm RMON form closes and the RMON (Create) form reappears.

10 Click on the Apply button.

11 Click on the Distribute button to manually distribute the policy locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

12 Close the RMON (Create) form. The Remote Network Monitoring (RMON) form reappears.

13 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

14 Close the Remote Network Monitoring (RMON) form.

56 — Constraint policies

56.1 Constraint policies overview *56-2*

56.2 Constraint policies procedures *56-2*

56.1 Constraint policies overview

Constraint policies regulate the number of records retained in the 5620 SAM database.

Size constraint policies

Size constraint policies regulate the number of historical records that the 5620 SAM database retains. The scheduling of tasks through the 5620 SAM can generate a great deal of archived result information if left unchecked. Size constraint policies control this volume by defining thresholds for various record classes. When the number of records for a specific class or group of classes reaches a threshold specified in the policy, the 5620 SAM deletes a specified number of the oldest objects that are associated with the class or group of classes.

Ageout constraint policies

Ageout constraint policies define a configurable ageout time for a specified object type meeting specified criteria, after which objects are deleted from the 5620 SAM database.

The 5620 SAM is pre-configured with a sample ageout constraint policy configured to delete inactive residential subscriber instance objects from the 5620 SAM database after the configured ageout time threshold has been exceeded. Residential subscriber instances become inactive in the 5620 SAM when the subscriber is deleted from the NE. The accumulation of inactive residential subscriber instances in the 5620 SAM database is particularly rapid under certain configurations (for example, Wi-Fi offload configurations).

56.2 Constraint policies procedures

The following procedures describe how to configure and manage constraint policies.

Procedure 56-1 To configure a size constraint policy

1 Choose Administration→Constraint Policies→Size Constraint Policies from the 5620 SAM main menu. The Size Constraint Policies form opens.

2 Perform one of the following:

   a Specify a filter to search for an existing policy. Select a policy in the filtered list and click on the Properties button.

   b Click on the Create button. The Size Constraint Policy (Create) form opens.

3 Configure the parameters:

- Auto-Assign ID
- Policy Id
- Description
- Threshold (# of objects)
- Objects To Be Deleted When Threshold Exceeded (# of objects)
- Apply Threshold To

4 Click on the Constrained Packages tab.

5 Right-click on the Size Constraint Policy icon and choose Select Packages from the contextual menu. The Select Size Constrained Packages form opens with a list of packages displayed.

6 Choose the packages to include in the size constraint policy and click on the OK button. The packages appear in the navigation tree under Constrained Packages.

7 From a package icon below the Size Constraint Policy icon, choose Select Classes from the right-click contextual menu to include in the size constraint policy.

   i Right-click on a package and choose Select Classes from the contextual menu. The Select Size Constrained Classes form opens.

   ii Choose the required classes in the list and click on the OK button. The classes appear in the navigation tree under the associated package.

8 Repeat step 7 for each package icon in the list.

9 Click on the OK button. The Size Constraint Policies form reappears with the new size constraint policy displayed in the list.

10 Close the Size Constraint Policies form.

Procedure 56-2 To configure an ageout constraint policy

Use this procedure to configure the descriptive text, administrative state, and ageout time for an existing ageout constraint policy. The 5620 SAM is preconfigured with an ageout constraint policy for inactive objects of the residential subscriber instance class.

1 Choose Administration→Constraint Policies→Ageout Constraint Policies from the 5620 SAM main menu. The Ageout Constraint Policies form opens.

2 Select a policy in the list and click on the Properties button. The Ageout Constraint Policy form opens.

3 Review the Object Count information displayed in the Status panel. This information refers to the most recent object deletion event, and may be useful in determining appropriate ageout time and deletion interval values for the policy.

4 Configure the parameters:

- Description
- Administrative State
- Qualified Ageout Time



Note — The default value for the Qualified Ageout Time parameter is 24 hours if the 5620 SAM is installed without the 5670 RAM, or 1464 hours with the 5670 RAM. The default value is not altered if the 5670 RAM is installed separately, but the value should be changed after a 5670 RAM install in order to maintain proper interoperability between the 5620 SAM and the 5670 RAM.

The default Qualified Ageout Time values should be regarded as generalized starting points for ageout time configuration (with or without a 5670 RAM install). Consider the following when setting the ageout time:

- A shorter ageout time prevents an excessively large residential subscriber instance table.
- The ageout time must be long enough to retain inactive subscriber instances for sufficient time to allow the upload of required information to third-party northbound applications.

5 If required, the read-only information in the Deletion Interval panel can be configured in the nms/config/AgeoutConstraintPolicy.xml file located on the 5620 SAM server.



Caution — Contact your Alcatel-Lucent technical support representative before you attempt to modify 5620 SAM server configuration files. Modifying the AgeoutConstraintPolicy.xml file can have serious consequences that can include service disruption.

i Open the AgeoutConstraintPolicy.xml file in a text editor.

ii Locate a block of code using the following syntax:

(Code 56-1shows deletion interval information for residential subscriber instances. Other object classes may also be defined in the file.)

Code 56-1: Deletion interval configuration

```
<ageout>
  <class name="ressubscr.ResidentialSubscriberInstance"
    ageoutSyncTime="00:00"
    ageoutInterval="1">
  </class>
</ageout>
```

iii Modify the values for ageoutSyncTime and ageoutInterval, as required.

iv Save and close the AgeoutConstraintPolicy.xml file.

v Execute the following command at the prompt:

```
bash$ ./nmsserver.bash read_config ↵
```

The changes in the AgeoutConstraintPolicy.xml file are loaded into the ageout constraint policy object.

6 Click on the OK button to close the Ageout Constraint Policy form, saving changes.

7 Close the Ageout Constraint Policies form.

57 — NAT policies

57.1 NAT policies overview *57-2*

57.1 NAT policies overview

A Network Address Translation (NAT) policy, defines general NAT properties and associates a NAT address pool with an ISA-NAT group on the same NE. A NAT policy is associated with a subscriber profile for L2-aware NAT in an IES or VPRN service, or for large-scale NAT in a VPRN service.

See chapter 24 for information about configuring and deploying NAT in a network.

58 — Format and range policies

58.1 Format and range policies overview *58-2*

58.2 Format and range policies procedures *58-5*

58.1 Format and range policies overview

The 5620 SAM supports format and range policies. Format policies manage how services, policies, LSPs, L2 and L3 access interfaces are named and described. Range policies manage the ID numbers that are assigned to services, policies, LSPs, L2 and L3 access interfaces. For example, you can configure a range policy to specify a range of 200 and 499 for all IDs for a service. You can configure a format policy to specify that service names do not exceed 10 characters. The object creation form indicates when a range or format policy is in effect for an object.

Format and range policies are not distributed to NEs. The format and range policies are configured when services, policies, LSPs, L2 and L3 access interfaces are created from the 5620 SAM GUI. You cannot configure format and range policies when the services, LSPs, L2 and L3 access interfaces are created using templates. However, the 5620 SAM allows an operator to use pre-configured examples of LSPs and services that have format and range policies applied to them. The examples can be used to create a template. For more information about creating templates from a pre-configured example, see "Format and range policies configuration of services and LSPs using templates" in the *5620 SAM Scripts and Templates Developer Guide*.

Table 58-1 lists the objects and associated parameters that can be managed using format and range policies.

Table 58-1 Format and Range policy objects and associated parameters

Object name	Format policy parameter	Range policy parameter
B-VPLS Service Site	Description, Name	—
Bypass-only LSP	Description, Name	ID
Customer	—	ID
Dynamic LSP	Description, Name	ID
I-VPLS Service Site	Description, Name	—
IES Group Interface	Description, Name	Interface ID
IES L3 Access Interface	Description, Name	Interface ID, Outer Encapsulation Value
IES Service	Description, Service Name	Service ID
IES Service Access Point	Description, Name	Outer Encapsulation Value
IES Service Site	Description, Name	—
IES Subscriber Interface	Description, Name	Interface ID
IP Mirror Interface	—	Interface ID
MVPLS B-L2 Access Interface	Description	Outer Encapsulation Value
MVPLS I-L2 Access Interface	Description	Outer Encapsulation Value
MVPLS L2 Access Interface	Description	Outer Encapsulation Value
MVPLS Service	Description, Service Name	Service ID
Mirror L2 Access Interface	—	Outer Encapsulation Value
MVPLS Service B-Site	Description, Name	—

(1 of 2)

Object name	Format policy parameter	Range policy parameter
MVPLS Service I-Site	Description, Name	—
MVPLS Service Site	Description, Name	—
Mirror Service	Description, Service Name	Service ID
Mirror Service Site	Description, Name	—
Redundant Interface	—	Interface ID
Spoke SDP Binding	—	VC ID
Static LSP	Description, Name	ID
Tunnel	Description, Name	ID
VLAN L2 Access Interface	Description	—
VLAN Service	Description, Service Name	Service ID
VLAN Service Access Point	Description, Name	—
VLAN Service Site	Description, Name	—
VLL Apipe Service	Description, Service Name	Service ID
VLL Apipe Service Site	Description, Name	—
VLL Cpipe Service	Description, Service Name	Service ID
VLL Cpipe Site	Description, Name	—
VLL Epipe Service	Description, Service Name	Service ID
VLL Epipe Service Site	Description, Name	—
VLL Fpipe Service	Description, Service Name	Service ID
VLL Fpipe Service Site	Description, Name	—
VLL Ipipe L2 Access Interface	Description	Outer Encapsulation Value
VLL Ipipe Service	Description	Service ID
VLL Ipipe Site	Description, Name	—
VLL L2 Access Interface	Description	Outer Encapsulation Value
VPLS B-L2 Access Interface	Description	Outer Encapsulation Value
VPLS I-L2 Access Interface	Description	Outer Encapsulation Value
VPLS L2 Access Interface	Description	Outer Encapsulation Value
VPLS L2 Management Interface	—	Interface ID
VPLS Service	Description, Service Name	Service ID
VPLS Service Site	Description, Name	—
VPRN Group Interface	Description, Name	Interface ID
VPRN L3 Access Interface	Description, Name	Interface ID, Outer Encapsulation Value
VPRN Service	Description, Service Name	Service ID
VPRN Service Access Point	Description, Name	Outer Encapsulation Value
VPRN Service Site	Description, Name	—
VPRN Subscriber Interface	Description, Name	Interface ID

(2 of 2)

Table 58-2 lists the policies that support format and range policies.

Table 58-2 Format and Range policy objects and associated parameters for policies

Policy	Format policy	Range policy
Access Ingress QoS	Description, Displayed Name	ID
Access Egress QoS	Description, Displayed Name	ID
ATM QoS policy	Description, Displayed Name	ID
Egress Queue Group template	Description, Displayed Name	—
7705 SAR Fabric Profile	Description, Displayed Name	ID
Policer Control policy	Description, Displayed Name	—
HSMDA Pool policy	Description, Displayed Name	—
HSMDA Scheduler policy	Description, Displayed Name	—
HSMDA WRED Slope policy	Description, Displayed Name	—
Ingress Queue Group template	Description, Displayed Name	—
MCFR Egress QoS Profile	Description	Profile ID
MCFR Ingress QoS Profile	Description	Profile ID
MLPPP Egress QoS Profile	Description	Profile ID
MLPPP Ingress QoS Profile	Description	Profile ID
Named Buffer Pool policy	Description, Name	—
Network policy	Description, Displayed Name	ID
Network Queue	Description, Name	—
Port Scheduler policy	Description, Displayed Name	—
Sap Access Ingress for 7210	Description, Displayed Name	ID
Network Policy for 7210	Description, Displayed Name	NW Mgr ID, Policy Id
Network Queue for 7210	Description, Name	—
Port Access Egress for 7210	Description, Displayed Name	ID
Port Scheduler for 7210	Description, Displayed Name	—
Slope Policy for 7210	Description, Displayed Name	—
Scheduler policy	Description, Displayed Name	—
WRED Slope policy	Description, Displayed Name	—
ACL IP filter	Description, Displayed Name	Filter ID
ACL IPv6 filter	Description, Displayed Name	Filter ID
ACL MAC filter	Description, Displayed Name	Filter ID
ANCP policy	Displayed Name	—
Host Tracking policy	Description, Displayed Name	—
MSAP policy	Description, Displayed Name	—
PPPoE policy	Description, Displayed Name	—
SLA Profile	Description, Displayed Name	—

(1 of 2)

Policy	Format policy	Range policy
Subscriber Explicit Map Entry	Description, Displayed Name	—
Subscriber Identification policy	Description, Displayed Name	—
Subscriber Profile	Description, Displayed Name	—
AA Application filter	—	Entry ID
Egress Multicast Group	Description, Displayed Name	—
Multicast Package	Description, Displayed Name	ID
Multicast CAC	Description, Name	—
Multicast PathMgmt BW policy	Description, Name	—
Multicast PathMgmt Info policy	Description, Name	—
AS Path	Description, AS Path Name	—
Community	Description, Community Name	—
Damping	Damping Name	—
Prefix List	Description, Prefix List Name	—
Statement	Description, Statement Name	—
MPLS Administrative Groups	Displayed Name	Value
Static Configuration for SRLGs	Displayed Name	—
Shared Risk Link Group Static Config	Displayed Name	Value
Accounting policy	Description, Displayed Name	ID
File policy	Description, Displayed Name	ID
Maintenance Domain	Description, Name	MD Mgr ID
Network Address Translation policy	Description, Displayed Name	—
PAE 802_1x policy	Description, Displayed Name	—
RADIUS Based Accounting	Description, Displayed Name	—
RMON	Description, Displayed Name	—
Time of Day Suite	Description, Name	—
Time Range	Description, Name	—
VRRP policy	Description, Displayed Name	ID, Service ID

(2 of 2)

58.2 Format and range policies procedures

The following procedures describe how to configure and manage format and range policies.

Procedure 58-1 To create or configure a format policy

Use this policy to specify the number and format of characters that can be used for text fields such as service names and descriptions.

1 Choose Administration→Format and Range Policies from the 5620 SAM main menu. The Format and Range Polices form opens.

2 Click on Format/Range (Property Rules). A navigation tree is displayed.

3 Click on Format Policy (Property Rules).

4 Perform one of the following:

a Click on the Search button to specify a filter to search for and modify a policy. A list of format policies is displayed. Go to step 5.

b Click on the Create button. The Format Policy (Create) form opens with the General tab displayed. Go to step 6.

5 Select a format policy in the list. The Format Policy (Edit) form opens with the General tab displayed.

6 Configure the parameters:

- Auto-Assign ID
- Policy ID
- Name
- Priority
- Administrative State

7 Click on the Select button beside the Object Type parameter. The Select Property - Format/Range Policy form opens.

8 Select an object for which you need to apply the name format policy.

9 Click on the OK button. The Select Property - Format/Range Policy form closes and the Format Policy (Create) or (Edit) form is updated with the object type.

10 Click on the Select button beside the Property Name parameter. The Select Property - Format/Range Policy form opens with a list of configurable properties for the object. The content of the list depends on the object that you specified in step 8.

11 Choose the property for which you need to apply the format policy and click on the OK button. The Select Property - Format/Range Policy form closes and Format Policy form is updated with property name.

12 Click on the Users tab.



Note — Only users and user groups that are assigned to this policy are affected by the policy. You can apply one or more format policies to a user or user group. See “5620 SAM user security tasks” in the *5620 SAM System Administrator Guide* for more information about creating users and user groups.

13 Click on the Add button. The Select User form opens with a list of users.

14 Select one or more users in the list and click on the OK button. The Format Policy form is refreshed with the selected users.

15 Click on the User Groups tab.

16 Click on the Add button. The Select Group form opens with a list of user groups.

17 Choose one or more user groups in the list and click on the OK button. The Format Policy (Create) or (Edit) form is refreshed with the selected user groups.

18 Click on the Text Block Formats tab to further define the format of the text. For example, an operator can classify a group of services with a similar name. The operator can also create a tool tip text to describe the purpose of the parameter.

19 Click on the Move Up or Move Down buttons to change the sequence of the text blocks in the text string.

20 Click on the Create button and perform one of the following:

a Choose Auto-Filled Parameter. The Auto-Filled Parameter (Create) form opens.

b Choose Masked Text Parameter. The Formatted Text (Create) form opens. Go to step 23.

c Choose Text Parameter. The Text (Create) form opens. Go to step 25.

21 Configure the parameters:

- Source Object Name
- Source Property Name
- Copy Text From Position
- Through To Position
- Displayed Text
- Tooltip Text

22 Go to step 26.

23 Configure the parameters:

- Mask
- Tooltip Text

24 Go to step 26.

25 Configure the parameters:

- Default Value
- Read Only
- Min. Length
- Max. Length
- Tooltip Text



Note — The Min. Length and Max. Length parameters are not configurable when the Read Only parameter is enabled.

26 Click on the OK button. A dialog box appears.

27 Click on the OK button. The Format Policy form reappears.

28 Click on the OK button. The Format Policy form closes.

29 Close the Format and Range Policies form.



Note — After a format policy is applied to a service, a combo box is displayed beside the object field during object creation, to indicate that a format policy is in effect. When there is only one matching policy, the combo box is dimmed. When there are multiple matching policies, the combo box is used to choose a policy. The sequence of the policies in the combo box is based on the value of the Priority parameter.

Procedure 58-2 To create or configure a range policy

Use this policy to specify the ID range for services, LSPs, L2 and L3 access interfaces.

1 Choose Administration→Format and Range Policies from the 5620 SAM main menu. The Format and Range Polices form opens.

2 Click on Format/Range (Property Values). A navigation tree is displayed.

3 Choose Range Policy (Property Rules).

4 Perform one of the following:

a Click on the Search button to specify a filter to search for and modify a policy. A list of range policies is displayed. Go to step 5.

b Click on the Create button. The Range Policy (Create) form opens with the General tab displayed. Go to step 6.

5 Select a range policy in the list. A Range Policy (Edit) form opens with the General tab displayed.

6 Configure the parameters:

- Auto-Assign ID
- Policy ID
- Name
- Priority
- Administrative State
- Minimum
- Maximum
- Auto Assignment Enabled
- Auto Assign By Default

7 Click on the Select button beside the Object Type parameter. The Select Property - Format/Range Policy form opens.

8 Select an object for which you need to apply the range policy.

9 Click on the OK button. The Select Property - Format/Range Policy form closes and the Range Policy (Create) form is updated with the object type.

10 Click on the Select button beside the Property Name parameter. The Select Property - Format/Range Policy form opens.

11 Choose the property for which you need to apply the range policy.

12 Click on the OK button. The Select Property - Format/Range Policy form closes and Range Policy (Create) form is updated with the property name.

13 Click on the Users tab.



Note — Only users and user groups that are assigned to this policy are affected by the policy. You can apply one or more range policies to a user or user group. See "5620 SAM user security tasks" in the *5620 SAM System Administrator Guide* for more information about creating users and user groups.

14 Click on the Add button. The Select User form opens with a list of users.

15 Choose one or more users in the list and click on the OK button. The Range Policy form is refreshed with the users.

16 Click on the User Groups tab.

17 Click on the Add button. The Select Group form opens with a list of user groups.

18 Choose one or more user groups in the list and click on the OK button. The Range Policy form is refreshed with the user groups.

19 Click on the OK button. The Range Policy form closes and the Format and Range Policies form reappears.

20 Close the Format and Range form.



Note — After a range policy is applied to a service, a combo box is displayed beside the object field during object creation, to indicate that a range policy is in effect. When there is only one matching policy, the combo box is dimmed. When there are multiple matching policies, the combo box is used to choose a policy. The sequence of the policies in the combo box is based on the value of the Priority parameter.

59 — PCP policies

59.1 PCP policies overview *59-2*

59.2 Workflow to configure and apply PCP policies *59-2*

59.3 PCP policies procedures *59-2*

59.1 PCP policies overview

PCP operates between subscribers and the NAT directly. This protocol provides the subscriber with limited but direct control over the NAT function. PCP configuration is supported on a Release 10.0 R4 or later 7750 SR.

PCP allows a customer to configure static port forwards, obtain information about existing port forwards and to obtain the outside IP address from software that runs on the home network or the CPE.

The PCP policy allows you to configure PCP parameters that affect the function of a NAT PCP server. The policy is applied to multiple NAT PCP servers so that they behave consistently.

59.2 Workflow to configure and apply PCP policies

1. Create a PCP policy. See Procedure 59-1 for more information.
2. Create a NAT PCP server. See Procedure 59-3 for more information about creating a NAT PCP server on the base routing instance. See Procedure 59-4 for more information about creating a NAT PCP server on a VPRN routing instance.
3. Associate an interface with the NAT PCP server. See Procedure 59-5 for more information.

59.3 PCP policies procedures

The following procedures describe how to configure, manage, and apply PCP policies.

Procedure 59-1 To create a PCP policy

1. Choose Policies→ISA Policies→NAT from the 5620 SAM main menu. The NAT Policies form opens.
2. Choose Port Control Protocol Policy (Network Address Translation) from the Select Object Type drop-down menu.
3. Click on the Create button. The PCP Policy, Global Policy (Create) form opens.
4. Configure the parameters:
   - Displayed Name
   - Description
   - Minimum Lifetime (seconds)
   - Maximum Lifetime (seconds)
   - Maximum Description Length

5 Configure the parameters in the Opcodes panel:

- Announce
- Get
- Map

6 Configure the parameters in the Options panel:

- Prefer Failure
- Port Reservation
- Description
- Third Party
- Next

7 Click on the Apply button. The PCP Policy, Global Policy (Edit) form opens with the General tab displayed.

8 Close the PCP Policy - Global Policy (Edit) form.

9 Close the NAT Policies form.

Procedure 59-2 To view a PCP policy

1 Choose Policies→ISA Policies→NAT from the 5620 SAM main menu. The NAT Policies form opens.

2 Choose Port Control Protocol Policy (Network Address Translation) from the Select Object Type drop-down menu.

3 Specify a filter to search for a profile, if required. Choose a profile from the list and click on the Properties button. The PCP Policy, Global Policy (Edit) form opens with the General tab displayed.

4 Click on the following tabs to view the properties of the policy, and the associated NEs, entities and faults.

- General—to view the general properties of the policy, such as the parameters configured in Procedure 59-1.
- Local Definitions—to view the NEs to which the policy is distributed.
- PCP Servers—to view the NAT PCP servers that are associated with the PCP policy.
- Faults—to identify faults and navigate to alarm information.

5 Close the NAT PCP Policy, Global Policy (Edit) form.

6 Close the NAT Policies form.

Procedure 59-3 To create a NAT PCP server on the base routing instance

1 Choose Routing from the navigation tree view selector. The navigation tree displays the routing view.

2 Expand a 7750 SR icon, right-click on the routing instance icon, and choose Properties from the contextual menu. The Routing Instance (Edit) form opens with the General tab displayed.

3 Click on the PCP Servers tab.

4 Click on the Create button. The Port Control Protocol Server (Create) form opens, with the General tab displayed.

5 Configure the following parameters:

- Name
- Description
- Administrative State

6 Click on the Select button for the Displayed Name parameter in the PCP Policy panel. The Select PCP Policy - Port Control Protocol Server form opens.

7 Choose a PCP policy from the list and click on the OK button. The Select PCP Policy - Port Control Protocol Server form closes.

8 Click on the Select button for the Routing Instance Name parameter in the Forwarding Inside Virtual Router panel. The Select Forwarding Inside Virtual Router - Port Control Protocol Server form opens.

9 Choose a routing instance from the list and click on the OK button. The Select Forwarding Inside Virtual Router - Port Control Protocol Server form closes.

10 Configure the Dual Stack Lite After Address parameter.

11 Click on the OK button. The Port Control Protocol Server (Create) form closes.

12 Close the VPRN Service (Edit) form.

13 Close the Manage Services form.

Procedure 59-4 To create a NAT PCP server on a VPRN routing instance

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria, if required. A list of services appears at the bottom of the Manage Services form.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

4 In the navigation tree, expand the Sites icon and click on the Routing Instance icon.

5 Click on the PCP Servers tab.

6 Click on the Create button. The Port Control Protocol Server (Create) form opens, with the General tab displayed.

7 Configure the following parameters:

- Name
- Description
- Administrative State

8 Click on the Select button for the Displayed Name parameter in the PCP Policy panel. The Select PCP Policy - Port Control Protocol Server form opens.

9 Choose a PCP policy from the list and click on the OK button. The Select PCP Policy - Port Control Protocol Server form closes.

10 Click on the Select button for the Routing Instance Name parameter in the Forwarding Inside Virtual Router panel. The Select Forwarding Inside Virtual Router - Port Control Protocol Server form opens.

11 Choose a routing instance from the list and click on the OK button. The Select Forwarding Inside Virtual Router - Port Control Protocol Server form closes.

12 Configure the Dual Stack Lite After Address parameter.

13 Click on the OK button. The Port Control Protocol Server (Create) form closes.

14 Close the VPRN Service (Edit) form.

15 Close the Manage Services form.

Procedure 59-5 To associate an interface with a NAT PCP server

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

4 In the navigation tree, expand the Sites icon and click on the Routing Instance icon.

5 Click on the PCP Servers tab.

6 Choose a server from the list and click on the Properties button. The Port Control Protocol Server (Create) form opens, with the General tab displayed.

7 Click on the Interfaces tab.

8 Click on the Create button. The Port Control Protocol Server Interface form opens.

9 Click on the Select button for the Interface Name parameter. The Select Interface - Port Control Protocol Server Interface form opens.

10 Choose an interface and click on the OK button.

11 Click on the OK button on the Port Control Protocol Server (Create) form. The form closes.

12 Close the VPRN Service (Edit) form.

13 Close the Manage Services form.

Procedure 59-6 To modify the interface associated with a NAT PCP server

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

4 In the navigation tree, expand the Sites icon and click on the Routing Instance icon.

5 Click on the PCP Servers tab.

6 Choose a server from the list and click on the Properties button. The Port Control Protocol Server (Create) form opens, with the General tab displayed.

7 Click on the Interfaces tab.

8 Click on an interface in the list. The Port Control Protocol Server Interface form opens, with the Interface Name parameter populated.

9 Click on the Select button for the Interface Name parameter. The Select Interface - Port Control Protocol Server Interface form opens.

10 Choose an interface, and click on the OK button. The Port Control Protocol Server Interface form opens with the Interface Name parameter populated with the new interface name.

11 Click on the OK button.

12 Click on the OK button.

13 Click on the Yes button. The Port Control Protocol Server (Edit) form closes.

Procedure 59-7 To modify the routing instance associated with the NAT PCP server

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

4 In the navigation tree, expand the Sites icon and click on the Routing Instance icon.

5 Click on the PCP Servers tab.

6 Choose a server from the list, and click on the Properties button. The Port Control Protocol Server (Edit) form opens with the General tab displayed.

7 Click on the Select button for the Routing Instance Name parameter. The Select Forwarding Inside Virtual Router - Port Control Protocol Server form opens.

8 Choose a routing instance from the list and click on the OK button. The Select Forwarding Inside Virtual Router - Port Control Protocol Server form closes. The Routing Instance Name parameter on the Port Control Protocol Server (Edit) form is populated.

9 Click on the Apply button on the Port Control Protocol Server (Edit) form.

10 Click on the Apply button on the VPRN Service (Edit) form.

11 Close the Manage Services form.

60 — Firewall policies

60.1 Overview of firewall policies on the 7705 SAR-H *60-2*

60.2 Workflow to configure and manage firewall policies on the 7705 SAR-H *60-4*

60.3 Configuring firewall policies for the 7705 SAR-H *60-4*

60.1 Overview of firewall policies on the 7705 SAR-H

The firewall supported on the 7705 SAR-H platform is a stateful firewall. A stateful firewall provides the highest level of security. Stateful operation is a key feature in preventing DoS attacks from reaching the TCP/IP stacks of applications.

You can configure firewall policies on the following firewall interfaces:

- layer 3 interfaces
- network interfaces
- management access interface
- CPM interface

To apply a firewall to an interface, you must configure entries with a firewall zone and IP address information.

The following components require configuration in order to implement a 7705 SAR-H firewall:

- Rules—packet matching actions, processing options, session management options, and NAT options which are required for a firewall security policy
- Rule Sets—the order list of rules that creates a firewall security policy when associated with a firewall zone. The rules are applied in order of precedence to packets that ingress or egress firewall zone configured interfaces
- Service Groups—a set of services (for example, IP protocol number, UDP/TCP ports) in the service matching field of a rule
- Host Groups—a collection of IP addresses and address ranges that may be optionally referenced in rule matching, NAT specifications, and other firewall functions
- Zones—define the security policy and are applied with a zone member IP address or range, to enable firewall protection for specified layer 3, router, management and CPM interfaces
- Zone member interfaces—the ingress or egress interfaces to which a firewall zone and zone-based IP address or IP address range has been applied. Firewall zones and related IP address information can be applied to layer 3, router, management and CPM interfaces

See the appropriate 7705 SAR-H documentation for more information.

Firewall zone management

A zone is a collection of hosts that share the same level of trust and access rights. Zones are named collections of interfaces, and their associated IP addresses or IP address ranges. A rule set of policies is defined for each zone and is used to determine actions to apply to packets that pass through zones. The following interfaces apply to a zone:

- VPRN SAP
- VPRN spoke-SDP
- IES SAP
- IES spoke-SDP

- network interface for non-VPRN traffic
- management access port
- CPM in-band traffic

An interface can have multiple entries in the same zone if the interface is expected to source multiple IP address ranges that require the same firewall policy. Similarly, the interface can have multiple entries in different zones if the interface is expected to source multiple IP address ranges that might require different firewall policies. An interface cannot overlap IP addresses or IP address ranges across the same or different zones, because the firewall requires a unique interface, IP address range tuple when searching for sessions. The 7705 SAR-H blocks overlapping configurations.

When you add an interface and IP address range tuple to a zone and the interface firewall is shut down, the change takes place immediately in the active firewall and packets are processed using the rule set for the configured zone firewall.



Note — Packets are only sent to the firewall if there is a route to a destination and the destination is reachable. If a packet cannot be routed because there is no route to a destination, or the destination is not reachable, or if the packet does not pass other checks like checksums, packet lengths, and so on, the packet is not sent to the firewall.

When you add an IP, SAP or spoke-SDP interface and IP Address range tuple to a zone, the change takes place immediately in the active firewall and packets are processed using the rule set configured for the zone. Packets ingressing and egressing the 7705 SAR-H firewall may not be configured on the ingress and egress interfaces, for example:

- zones configured on ingress and egress interfaces: The 7705 SAR-H sends the packet to the firewall and applies the ingress zone rule set to the packet. If the packet passes the ingress zone rules, the firewall applies the egress zone rule set to the packet. If the packet passes the egress zone rules, the packet is forwarded out of the egress interface. The packet is dropped for all other scenarios.
- zones configured on ingress interface only: The 7705 SAR-H sends the packet to the firewall and applies the ingress zone's rule-set to the packet. If the packet passes the ingress zone rules, the packet is forwarded out of the egress interface.
- zones configured on egress interface only: On receipt of the packet on the ingress interface, the 7705 SAR-H determines the egress zone and whether there is a zone configured. If there is a zone configured, the packet is sent to the firewall and applies the egress zone rule set to the packet. If the packet passes the rules, the packed is forwarded out of the egress interface.
- zones not configured on both ingress or egress interface: The 7705 SAR-H does not send the packet to the firewall processor, and the packet is processed using the network processor only.

60.2 Workflow to configure and manage firewall policies on the 7705 SAR-H

1. Distribute a license key to all 7705 SAR-H nodes. See "5620 SAM component configuration overview" in the *5620 SAM System Administrator Guide* for more information.
2. Configure a host group firewall policy. See Procedure 60-1.
3. Configure a service group firewall policy. See Procedure 60-2.
4. Configure a rule set firewall policy. See Procedure 60-3.
5. Configure a zone firewall policy. See Procedure 60-4.
6. Configure a firewall log policy. See Procedure 60-5.
7. Configure an NE firewall using the firewall manager. See "Configuring a firewall on a 7705 SAR-H using the firewall manager" in the *5620 SAM System Administrator Guide* for more information.
8. Configure an NE management access firewall using the firewall manager. See "Configuring a firewall on a 7705 SAR-H management access or CPM interface" in the *5620 SAM System Administrator Guide* for more information.
9. Configure an NE CPM firewall using the firewall manager. See "Configuring a firewall on a 7705 SAR-H management access or CPM interface" in the *5620 SAM System Administrator Guide* for more information.

60.3 Configuring firewall policies for the 7705 SAR-H

Perform the following procedures to configure firewall policies for the 7705 SAR-H.

Procedure 60-1 To configure a host group firewall policy

The 5620 SAM supports the 7705 SAR-H host group policy that provides a rule that allows multiple IP addresses to be included in a policy.

- The 5620 SAM manages the host group as a policy under the firewall.
- The 5620 SAM allows configuration of host groups from a common firewall manager.



Note 1 — Host groups are referred to in rule sets, for example, NAT hostgroup IP.

Note 2 — Configuration can be for a standard policy or local instance (non-policy) configuration.

1. Choose Policies→Firewall from the 5620 SAM main menu. The Firewall Policies form opens.
2. Choose Host Group (Firewall) from the Select Object Type drop-down menu.

3 Perform one of the following:

a Choose Create→Host Group option from the drop-down menu.The Host Group form opens with the General tab displayed.

b Specify a filter to search for and modify a policy. Choose a policy from the filtered list and click on the Properties button. The Host Group form opens with the General tab displayed.

4 Configure the parameters:

- Auto-Assign ID (ID is disabled if Auto-Assign ID is chosen)
- ID
- Displayed Name
- Description

5 Click on the Host Group Entries tab.

6 Click on the Create button. The Host Group Entry form opens.

7 Configure the parameters:

- Auto-Assign ID (Entry ID is disabled if Auto-Assign ID is chosen)
- Entry ID
- Displayed Name
- Description

8 In the IP Address panel, select the IP Operator check box. Choose one of the following options from the drop-down menu and enter the IPv4 address (using the following format d.d.d.d):

- EQUAL
- RANGE

9 Click on the OK button. The Host Group form opens.

10 Click on the OK button to save the changes and close the Host Group form. The Firewall Policies form opens.

11 Choose the newly created Host Group policy and click on the Properties button.

12 The Host Group form opens. The Configuration Mode parameter in the Policy Configuration panel is in the Draft state. Release the policy and distribute the policy as required.

i Click on the Switch Mode button. A confirmation dialog box opens.

ii Click on the Yes button to confirm the action. The Configuration Mode is changed to Released state.

13 When you release the global policy, the policy is also distributed to existing local definitions. See chapter 42 for information about how to distribute a policy.



Note 1 — You can choose a policy from the Firewall Policies form and click on the Delete button to delete the policy.

Note 2 — Policies can be deleted in the following order:

- Zone
- Rule Set
- Host Group or Service Group

Note 3 — Host Group or Service Group policies cannot be deleted if rule sets are associated with them.

Note 4 — Rule set policies cannot be deleted if they are associated with zones.

Note 5 — Zone policies cannot be deleted if they are associated with SAP, SDP, MGMT, or CPM interfaces.

Procedure 60-2 To configure a service group firewall policy

The 5620 SAM supports the 7705 SAR-H host group that provides a rule that represents services (protocols, ports, protocol families) to be included in a policy.

- The 5620 SAM manages the service group as a policy in the firewall.
- The 5620 SAM allows configuration of service groups from a common firewall manager.



Note 1 — Service groups are referred to in rule sets, for example, NAT 'hostgroup IP.

Note 2 — Configuration can be a standard policy or local instance (non-policy) configuration.

1 Choose Policies→Firewall from the 5620 SAM main menu. The Firewall Policies form opens.

2 Choose Service Group (Firewall) from the Select Object Type drop-down menu.

3 Perform one of the following:

a Choose Create→Service Group option from the drop-down menu. The Service Group form opens with the General tab displayed.

b Specify a filter to search for and modify a policy. Choose a policy from the filtered list and click on the Properties button. The Service Group form opens with the General tab displayed.

4 Configure the parameters:

- Auto-Assign ID (ID is disabled if Auto-Assign ID is chosen)
- ID
- Displayed Name
- Description

5 Click on the Service Group Entries tab.

6 Click on the Create button. The Service Group Entry form opens.

7 Configure the parameters:

- Auto-Assign ID (Entry ID is disabled if Auto-Assign ID is chosen)
- Entry ID
- Displayed Name
- Description

8 In the Protocol panel, choose a protocol from the drop-down menu and configure one of the following:

a Choose ICMP (1). The ICMP Properties panel is displayed.

i Select the ICMP Code check box.

ii Choose a code from the drop-down menu.

iii Choose an ICMP Type from the drop-down menu.

b Choose IGMP (2). The IGMP panel is displayed.

i Select the IGMP Type check box.

ii Choose a type from the drop-down menu.

c Choose UDP (17). The Port Properties panel is displayed.

i Select the Source Port check box and choose an option from the drop-down menu.

ii Select the Dest Port check box and choose an option from the drop-down menu.

d Choose TCP (6). The Port Properties panel is displayed.

i Select the Source Port check box and choose an option from the drop-down menu.

ii Select the Dest Port check box and choose an option from the drop-down menu.

e Choose any other protocol.

9 Click on the OK button. The Service Group form opens.

10 Click on the OK button to save the changes. The Firewall Policies form opens.

11 Choose the newly created Service Group firewall policy and click on the Properties button.

12 The Service Group form opens. The Configuration Mode parameter in the Policy Configuration panel is in the Draft state. Release the policy and distribute the policy as required.

i Click on the Switch Mode button. A confirmation dialog box opens.

ii Click on the Yes button to confirm the action. The Configuration Mode is changed to Released state.

13 When you release the global policy, the policy is also distributed to existing local definitions. See chapter 42 for information about how to distribute a policy.



Note 1 — You can choose a policy from the Firewall Policies form and click on the Delete button to delete the policy.

Note 2 — Policies can be deleted in the following order:

- Zone
- Rule Set
- Host Group or Service Group

Note 3 — Host Group or Service Group policies cannot be deleted if a rule set are associated with them.

Note 4 — Rule set policies cannot be deleted if they are associated with zones.

Note 5 — Zone policies cannot be deleted if they are associated with SAP, SDP, MGMT, or CPM interfaces.

Procedure 60-3 To configure a rule set firewall policy

The 5620 SAM supports the 7705 SAR-H rule set policy that provides a rule that represents a complex set of restrictions, for example, an ACL. A rule set can refer to the service or host group policies.

- The 5620 SAM manages the rule set as a policy under the firewall.
- The 5620 SAM allows configuration of rule sets from a common firewall manager.



Note 1 — Host groups are referred to in rule sets, for example, NAT hostgroup IP.

Note 2 — The Zone Associations tab displays the zones that are associated with the rule sets.

Note 3 — Configuration can be for a standard policy or local instance (non-policy) configuration.

1 Choose Policies→Firewall from the 5620 SAM main menu. The Firewall Policies form opens.

2 Choose Rule Set (Firewall) from the Select Object Type drop-down menu.

3 Perform one of the following:

a Choose Create→Rule Set option from the drop-down menu. The Rule Set form opens with the General tab displayed.

b Specify a filter to search for and modify an existing policy. Choose a policy from the filtered list and click on the Properties button. The Rule Set form opens with the General tab displayed.

4 Configure the parameters:

- Auto-Assign ID (ID is disabled if Auto-Assign ID is chosen)
- ID
- Displayed Name
- Description

5 Click on the Rule Set Entries tab.

6 Click on the Create button. The Rule Set Entry form opens.

7 Configure the following parameters:

- Auto-Assign ID (Entry ID is disabled if Auto-Assign ID is chosen)
- Entry ID
- Displayed Name
- Description
- Action
- Forwarding Role

8 If the Forwarding Role parameter is configured as Source or Destination, the NAT tab is enabled. Click on the NAT tab.

9 In the Source Host panel, configure one of the following:

- **a** Select the Source IP check box and enter an IPv4 address.
- **b** Select the Source Host Group check box and configure the following:
  - **i** Click on the Select button to choose a source host group ID.
  - **ii** The Select Source Host Group form opens.
  - **iii** Click on the Search button to choose a source host group ID from the list, or click on the Create button; the Host Group form opens. See Procedure 60-1.
  - **iv** Click on the OK button. The Rule Set Entry form opens.

10 In the Destination Host panel, configure one of the following:

- **a** Select the Destination IP check box and enter an IPv4 address.
- **b** Select the Destination Host Group check box and configure the following:
  - **i** Click on the Select button to choose a destination host group ID.
  - **ii** The Select Destination Host Group form opens.
  - **iii** Click on the Search button to choose a destination host group ID from the list, or click on the Create button, the Host Group form opens. See Procedure 60-1.
  - **iv** Click on the OK button. The Rule Set Entry form opens.

11 In the Service Group panel:

- **i** Click on the Select button to choose a service group ID.
- **ii** The Select Service Group form opens.
- **iii** Click on the Search button to, choose a service host group ID from the list, or click on the Create button, the Service Group form opens. See Procedure 60-2.
- **iv** Click on the OK button. The Rule Set Entry form opens.

12 Click on the Match Criteria tab and configure the parameters.

13 In the Criteria panel, configure one of the following:

a Select the Protocol check box and choose one of the protocols from the drop-down menu.



Note 1 — Based on the protocol chosen, you can configure additional properties. See Procedure 60-2, step 8.

Note 2 — In the Match Criteria tab, if the protocol chosen is TCP/UDP/NONE, then Source Port, Destination Port, and Service Group options are displayed in the NAT tab. See steps 9 to 11.

b Select the Service Group check box and configure the following:

i Click on the Select button to choose a service group ID.

ii The Select Service Group form opens.

iii Click on the Search button to choose a Service Group ID from the list, or click on the Create button, the Service Group form opens. See Procedure 60-2.

iv Click on the OK button. The Rule Set Entry form opens.

14 In the IP panel, choose one of the following options to configure the source IP:

a Select the Source IP check box and enter an IPv4 address.

b Select the Source Host Group check box and configure the following:

i Click on the Select button to choose a source host group ID.

ii The Select Source Host Group form opens.

iii Click on the Search button to choose a source host group ID.

iv Click on the OK button. The Rule Set Entry form opens.

15 From the IP panel, choose one of the following to configure the destination IP:

a Select the Destination check box and enter an IPv4 address.

b Select the Destination Host Group check box and configure the following:

i Click on the Select button to choose a destination host group ID.

ii The Select Destination Host Group form opens.

iii Click on the Search button, to choose a Destination Host Group ID

iv Click on the OK button. The Rule Set Entry form opens.

16 Click on the Options tab.

17 Configure the following parameters by clicking on the check box:

- Max Concurrent Sessions
- Session Timeout
- IP Option (hex)
- Strict TCP
- Session Reverse Direction

18 Click on the check box in the Log Id panel and configure the ID.

i Click on the Select button.

ii The Select Log Id form opens.

iii Click on the Search button to display the log IDs.

iv Choose a log ID and click on the OK button.

v The Rule Set form opens.

19 Click on the OK button to save the changes and close the Rule Set form. The Firewall Policies form opens.

20 Choose the newly created Rule Set firewall policy and click on the Properties button.

21 The Rule Set form opens with the General tab displayed. The Configuration Mode parameter in the Policy Configuration panel is in the Draft state. Release the policy and distribute the policy as required.

i Click on the Switch Mode button. A confirmation dialog box opens.

ii Click on the Yes button to confirm the action. The Configuration Mode is changed to Released state.

22 When you release the global policy, the policy is also distributed to local definitions. See chapter 42 for information about how to distribute a policy.

23 Click on the Rule Set Entries tab.

24 Click on the Search button to display the rule set entries.

25 Choose an entry from the list and click on the Renumber ID button.

26 The Renumber Entry ID form opens.

27 Enter the New Entry ID. Click on the OK button to close the form and return to the Rule Set form.



Note 1 — You can choose a policy from the Firewall Policies form and click on the Delete button to delete the policy.

Note 2 — Policies can be deleted in the following order:

- Zone
- Rule Set
- Host Group or Service Group

Note 3 — Host Group or Service Group policies cannot be deleted if rule sets are associated with them.

Note 4 — Rule set policies cannot be deleted if they are associated with zones.

Note 5 — Zone policies cannot be deleted if they are associated with SAP, SDP, MGMT, or CPM interfaces.

Procedure 60-4 To configure a zone firewall policy

The 5620 SAM supports the 7705 SAR-H zone policy rules with two modes of operation within the firewall manager. A rule allows services (protocols, ports, and protocol families) to be included in a policy.



Note 1 — Zones are referred to in rule sets, for example, a network rule set or service-facing rule set.

Note 2 — Configuration of zone policies can be for a standard policy or a local instance (non-policy) configuration.

1 Choose Policies→Firewall from the 5620 SAM main menu. The Firewall Policies form opens.

2 Choose Zone (Firewall) from the Select Object Type drop-down menu.

3 Perform one of the following:

a Choose Create→Zone option from the drop-down menu. The Zone form opens with the General tab displayed.

b Specify a filter to search for and modify a policy. Choose a policy from the filtered list and click on the Properties button. The Zone form opens with the General tab displayed.

4 Configure the parameters:

- Auto-Assign ID (ID is disabled if Auto-Assign ID is chosen)
- ID
- Displayed Name
- Description

5 Click on the Zone Entries tab.

6 Click on the Create button. The Zone Entry form opens.

7 Configure the parameters:

- Auto-Assign ID (Entry ID is disabled if Auto-Assign ID is chosen)
- Entry ID
- Displayed Name
- Description

8 Click on the Select button on the Zone Entry form. The Select Rule Set form opens.

9 Perform one of the following:

a Click on the Search button to display the rule set IDs.

b Click on the Create button. The Rule Set form opens. See Procedure 60-3.

10 Choose an ID from the list and click on OK. The Zone Entry form opens.

11 Click on the OK button. The Zone form opens.

12 Click on the OK button to save the changes and close the Zone form. The Firewall Policies form opens.

13 Choose the newly created Zone firewall policy and click on the Properties button.

14 The Zone form opens with the General tab displayed. The Configuration Mode parameter in the Policy Configuration panel is in the Draft state. Release the policy and distribute the policy as required.

i Click on the Switch Mode button. A confirmation dialog box opens.

ii Click on the Yes button to confirm the action. The Configuration Mode is changed to Released state.

15 When you release the global policy, the policy is also distributed to local definitions. See chapter 42 for information about how to distribute a policy.

16 Click on the Zone Entries tab.

17 Click on the Search button to display the zone entries.

18 Choose an entry from the list and click on the Renumber ID button.

19 The Renumber Entry ID form opens.

20 Enter the New Entry ID. Click on the OK button to close the form and return to the Zone form.

Note 1 — You can choose a policy from the Firewall Policies form and click on the Delete button to delete the policy.

Note 2 — Policies can be deleted in the following order:

- Zone
- Rule Set
- Host Group or Service Group

Note 3 — Host Group or Service Group policies cannot be deleted if a rule sets are associated with them.

Note 4 — Rule set policies cannot be deleted if they are associated with zones.

Note 5 — Zone policies cannot be deleted if they are associated with SAP, SDP, MGMT, or CPM interfaces.

Procedure 60-5 To configure a firewall log policy

You can configure a firewall log policy and associate it with a rule set.

Note — You cannot attach a zone containing a ruleset that has a firewall log with destination as syslog to the management access firewall.

1 Choose Policies→Log Configuration. The Manage Log Configuration Policies form appears.

2 Perform one of the following:

a Specify Firewall Log (Node Log Policy) and click on the Search button to search for an existing firewall log. Select a policy in the filtered list and click on the Properties button. The Firewall Log, Global Policy (Edit) form opens with the General tab displayed.

b Click on the Create button and select Firewall Log from the menu. The Firewall Log, Global Policy (Create) form appears.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Log Description
- Log Destination
- Maximum Number of Entries
- SysLog Id
- Log Stop On Full
- Log Enabled
- Log Summary Enabled
- Log Summary Criterion

The SysLog Id, Log Summary Enabled, and Log Summary Criterion parameters are only configurable when you choose the SysLog option as the Log Destination. Perform steps 4 to 8.

The Maximum Number of Entries parameter is only configurable when you choose the Memory option as the Log Destination.

4 If you choose SysLog as the Log Destination, click on the Select button to select a SysLog ID. The Select SysLog ID - Firewall Log ID form appears.

5 Click on the Search button to display a list of SysLog IDs.

6 Select a SysLog ID from the list and click on the OK button. The Firewall Log form reappears.

7 Click on the Apply button. A dialog box appears.

8 Click on the Yes button. The Policy Configuration panel is displayed.

9 Click on the Switch Mode button to distribute the policy to the required NEs. A dialog box appears. Click on the Yes button. The Release - Firewall Log form appears.



Note — When the policy is in draft mode the Distribute button under the More Actions button is dimmed, and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Release Firewall Log form, where you can select which NEs to distribute the policy to. See chapter 42 for more information.

10 Select the required NEs from the list of Available Objects on the left and move them to the Selected Objects list on the right using the right-pointing arrow.

11 Click on the Distribute button. The Status field in the Selected Objects list provides the status of the distribution.

12 Close the Release - Firewall Log form.

13 Close the Firewall Log form.

Service management

61 — Service management and QoS

62 — Queue groups

63 — Virtual ports

64 — Customer configuration and service management

65 — Residential subscriber management

66 — VLAN service management

67 — VLL service management

68 — VPLS management

69 — Mirror service management

70 — IES management

71 — VPRN service management

72 — PW routing and dynamic MS-PW service management

73 — Service PW template policy management

74 — Composite service management

75 — Dynamic service management

76 — Application assurance

77 — Service Test Manager

78 — Ethernet CFM

79 — Tunnel administrative groups

80 — RCA audit

81 — Service throughput configuration

61 — Service management and QoS

61.1 Service management and QoS overview *61-2*

61.2 5620 SAM and the triple play service delivery architecture *61-12*

61.3 BTV multicast configuration examples *61-22*

61.4 Sample network configuration using QoS *61-29*

61.5 Sample SAP QoS configuration *61-31*

61.6 Workflow to implement QoS on an OmniSwitch *61-39*

61.7 Workflow to implement QoS on the 7750 SR, 7450 ESS, 7710 SR, 7705 SAR, and 7950 XRS *61-40*

61.8 5620 SAM QoS policies *61-41*

61.1 Service management and QoS overview

The 5620 SAM supports the configuration of the following network services:

- VLL service
- VPLS / MVPLS / HVPLS
- IES
- VPRN service
- VLAN service
- composite service
- mirror service

A 5620 SAM operator can create, configure and delete services on sites and routers that are within their span of control.

The benefits of the 5620 SAM service model include:

- service creation using configuration forms or preconfigured XML API template; see "XML API template administration" in the *5620 SAM Scripts and Templates Developer Guide* for information about creating and using XML API templates
- service management using configuration forms and a navigation tree
- linking of services to create composite services that support complex customer applications
- policies that specify the NE traffic classification, policing, shaping, time of day restrictions, and marking
- traffic management capabilities to customize the delivery of different services according to SLAs
- integrated fault management functions

Customer traffic enters a service through one or more access interfaces. In a local service, all access interfaces are on one NE. In a distributed service, multiple NEs are deployed at the PE. Customer traffic is transported across an IP/MPLS core network in unidirectional service tunnels that use GRE or MPLS LSPs. Many services can use the same tunnel. Figure 61-1 shows an example of a distributed VLL service.

Figure 61-1 Distributed VLL service

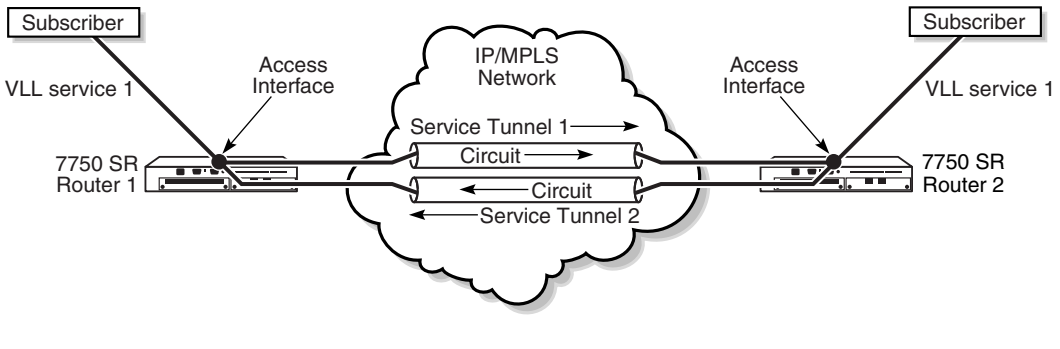
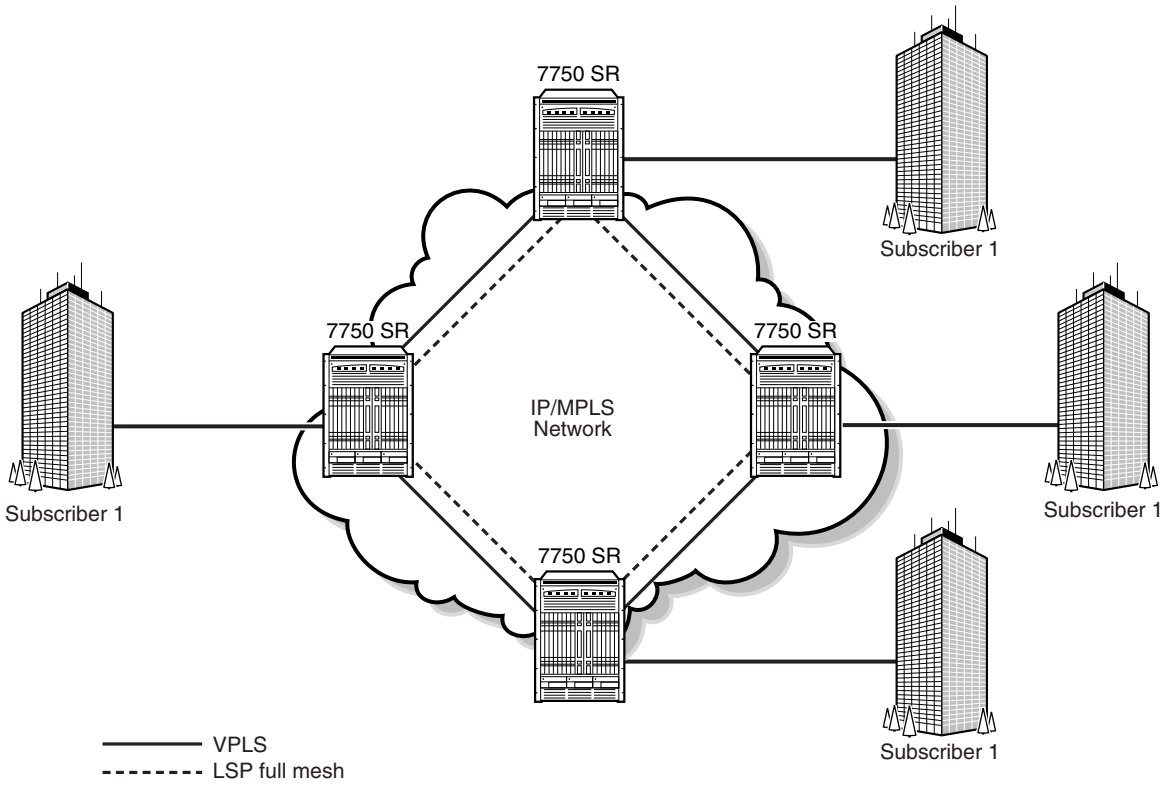


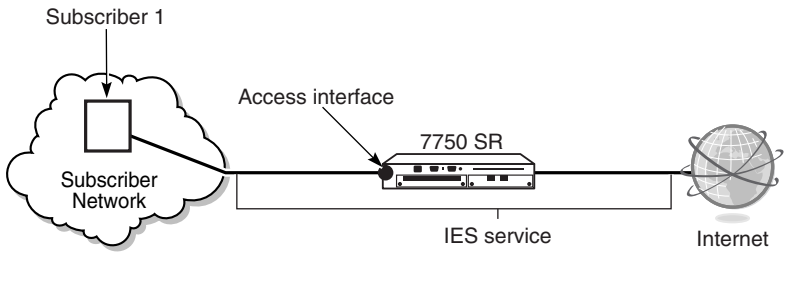
Figure 61-2 shows an example of a distributed VPLS.

Figure 61-2 Distributed VPLS



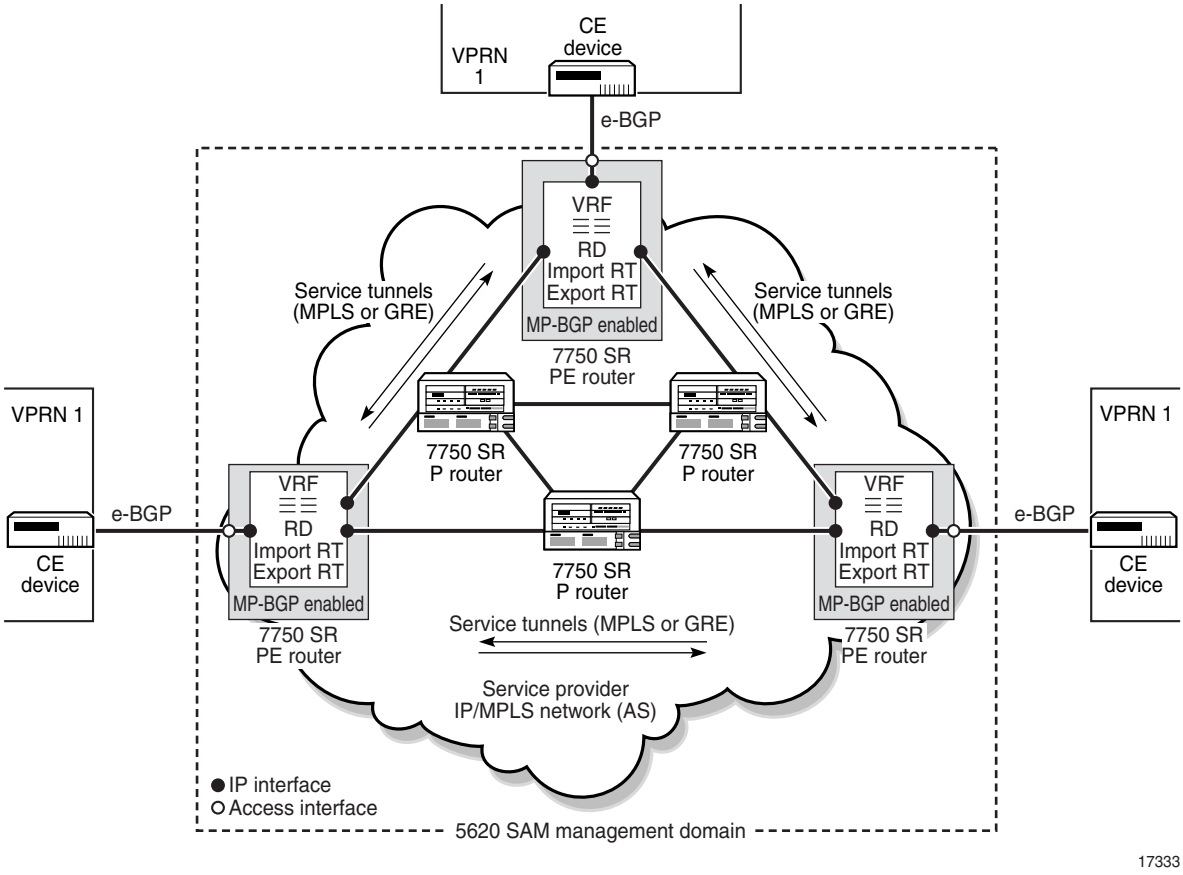
For IES, the managed devices are deployed at the provider edge and customer traffic enters the service using access interfaces. IES is a routed connectivity service where the customer communicates with an IP router interface to send and receive Internet traffic. Figure 61-3 shows a sample IES.

Figure 61-3 Sample IES



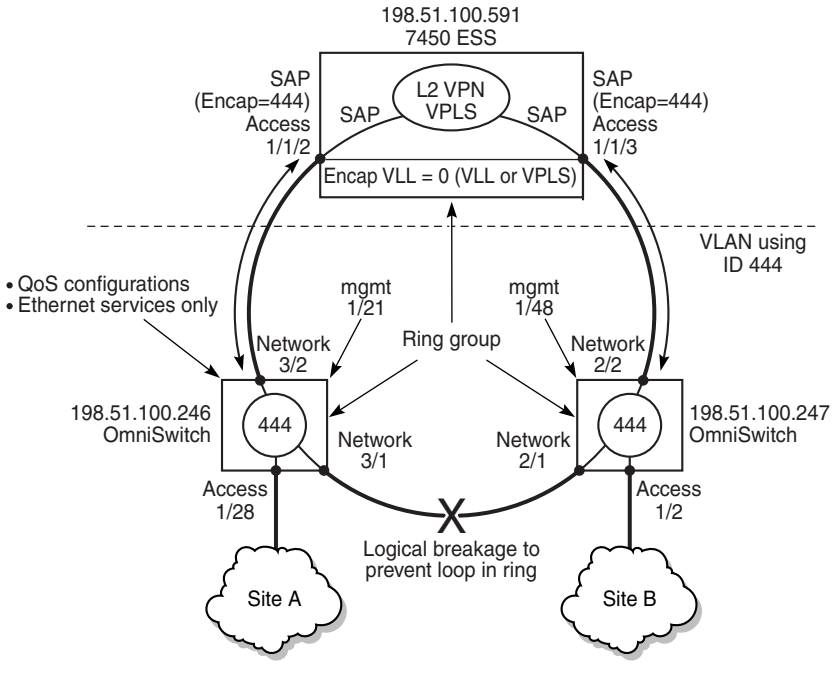
For VPRN services, the managed devices can be deployed as PE or provider core routers. Data and distribution of routing information are forwarded across an IP/MPLS service provider core network. Figure 61-4 shows a sample VPRN service.

Figure 61-4 Sample VPRN service



VLAN ring groups are used to send traffic across an Ethernet ring using copper or fiber optic connections from the source traffic device, for example, a 7450 ESS, to all devices in the ring. Any breaks in the physical links between devices are rerouted. Figure 61-5 shows a sample VLAN for L2 VPNs.

Figure 61-5 Sample VLAN configuration for L2 VPNs



A composite service allows the interconnection of different service types to form a service delivery network that is tailored to a specific application. For example, VPRN, VPLS, and VLAN services can be joined to create a routed multicast TV distribution mechanism that spans a wide geographical area.

A mirror service is a unidirectional service function that duplicates a specified traffic stream and sends the duplicate stream to a monitoring device for troubleshooting or surveillance purposes. With pseudo-wire redundancy support, an ICB can be enabled in a mirror service spoke and a remote source, which can provide bidirectional service that enables support for active and standby PE redundancy.

QoS provides the ability to rate limit across multiple queues from one or more access interfaces for a customer, and to differentiate service levels for different types of traffic. For higher priority traffic such as VoIP or video, you can specify reserved bandwidth. Lower priority applications, such as data traffic, may not have reserved bandwidth but can burst to use all the available bandwidth.

The main elements of QoS are:

- QoS markings

  Customer traffic may be marked with QoS markings, such as DSCP, EXP, and dot1p, that are mapped to forwarding classes.

  All forwarding classes support profile marking of packets as in-profile or out-of-profile. In-profile packets have a high enqueuing priority. Out-of-profile packets have a low enqueuing priority. Profile marking of packets can occur at two points: when packets are classified into forwarding classes at access ingress and when packets are classified at service egress. Profile marking is only done on the internal header and not in an actual encapsulation.

- forwarding classes
  Provide network elements with a method to weigh the relative importance of packets, only in relation to other forwarding classes. A forwarding class is also referred to as a Class of Service.
- queues
  Location for buffering packets that are to be forwarded before they are scheduled.
- schedulers
  Hardware scheduling (or single-tier scheduling) exists by default on a device and consists of a high-priority and a low-priority scheduler.
  Scheduler policies (or multi-tier scheduling) provide a more complex, hierarchical structure of virtual schedulers that override the default hardware behavior for more flexible scheduling capabilities.
- slope policies
  Define the WRED slope characteristics of hardware buffer space that is used by the ingress and egress queues

See chapter 42 for more information about policies on the 5620 SAM. See the *7750 SR OS Services Guide* for more detailed information about QoS.

Access interfaces

Each customer service is configured with at least one access interface point called a SAP. The access interface identifies the point of customer interface for a service on the managed device.

A Layer 2 or Layer 3 access interface is uniquely identified using these parameters:

- physical Ethernet port or POS port and channel
- encapsulation type (if applicable)
- encapsulation id (if applicable)

Depending on the encapsulation type, a physical port or channel can have more than one access interface associated with it. Using encapsulation or a SONET/SDH channel, devices can support multiple services for a customer or for multiple customers.

Access interfaces can only be created on ports or channels that are designated as access in the physical port configuration. Access interfaces cannot be created on ports designated as core-facing network ports because these ports have a different set of features enabled in software.

Access interfaces can participate in policies. Time of day suites can also be associated with access interfaces to apply a set of time-based policies, filters, and schedulers. Configuration of access interfaces can be performed during service configuration or modification. When you configure an access interface, consider the following:

- An access interface is owned by and associated with the service in which it is created.
- An access interface is a local entity and is locally unique to a specific device. The same access interface ID value can be used on another device.
- There are no default access interfaces. All access interfaces must be created.

- The default administrative state for an access interface at creation time is administratively enabled.
- If a port or channel is shut down (administratively or operationally), access interfaces on that port/channel are operationally out of service.

Automatic SDP (service tunnel) binding for services

You configure automatic service tunnel (SDP) binding for services when you configure a service using configuration forms or templates.

The 5620 SAM defines its own internal rules on how automatic mesh SDP bindings are performed.

1 The 5620 SAM tries to find the least-used SDP (service tunnel) with the lowest load factor (the lower the number of bindings, the lower the load factor) from the source to destination NE when the service tunnel meets the following conditions:
   - the service tunnel operational state is up
   - the operational MTU is greater than or equal to the MTU value of the service site
   - T-LDP is set for SDP bindings of VPLS, IES, or VLL services
   - the selected transport method, either GRE, LDP, or RSVP
2 When no service tunnel operational state is up, 5620 SAM tries to find the least-used service tunnel with the lowest load factor in an operationally down state.
3 For mirror services, binding are created from the source sites to the destination sites.
4 When a service tunnel cannot be found for a service site, a change in the site leads to another search. For example, if the service MTU is 1500 and the highest path MTU in all SDPs from that site is 1472, no SDP binding can be successful. If the service MTU is lowered to 1472 or less, a successful SDP binding results.
5 When a service tunnel is not found, and the transport method selected is GRE, 5620 SAM attempts to create a GRE service tunnel with a path MTU equal to the service site service MTU with T-LDP signaling turned on.

See "MTU size and port configuration" in section 16.2 for more information on MTU size considerations.

Multi-segment tunnel selection

Multi-segment tunnel selection functionality enhances tunnel selection functionality to allow the system to select intermediate NEs in a path, as well as the service tunnels from a selected intermediate NE to its next hop. Multi-segment tunnel selection functionality is used to select existing SDPs. It cannot create new SDPs.

Tunnels are selected based on the following criteria:

- If a metric value is specified for any of the SDPs along the path, the path with the lowest sum of the metric property for all SDPs along the path is selected.
- If no metric is specified for any of the SDPs along the path, the path with the fewest number of SDPs (hops) is selected.
- If two paths or SDPs are equal based on the selection criteria mentioned above, the SDP/path with the lowest load factor (number of services using that SDP) is selected.

Multi-segment tunnel selection functionality must be enabled at the system level, as well as at the tunnel selection profile level. Table 61-1 describes the objects to which a tunnel selection profile with multi-segment tunnel selection can be assigned, and the service tunnel configurations that result.

Table 61-1 Multi-segment tunnel selection scenarios

Tunnel selection profile applied to...	Resulting tunnel configuration
Spoke SDP binding on a VLL service	This scenario applies to a VLL service with two terminating sites. One of the sites has a spoke SDP binding configured with Auto-Select Transport Tunnel enabled, and a tunnel selection profile with Multi-segment Tunnel Selection enabled. If a valid path is found between the two terminating sites, the spoke SDP bindings and switching sites are created.
VLL service	This scenario applies to a VLL service with two terminating sites. The service is configured with Automatic SDP Binding/PBB Tunnel Creation enabled, and a tunnel selection profile with Multi-segment Tunnel Selection enabled. If a valid path is found between the two terminating sites, the spoke SDP bindings and switching sites are created.
Spoke termination point	This scenario applies to a spoke SDP binding between any two supporting objects. These include (M-)VPLS sites, (M-)VPLS I-sites, (M-)VPLS B-sites, VLL sites, IES L3 access interfaces, VPRN L3 access interfaces, VLL endpoints, and VPLS endpoints. The spoke SDP binding is configured with Auto-Select Transport Tunnel enabled, and a tunnel selection profile with Multi-segment Tunnel Selection enabled. If a termination point is specified, the spoke SDP bindings and return spoke SDP bindings are created. Switching sites are created as follows: • If the spoke SDP binding is created on a VLL service, the switching sites are created on the VLL service. • If the specified termination point is on a VLL service, the switching sites are created on the VLL service. • If neither end of the tunnel is on a VLL service, a new EPIPE service is created. The service component ID is auto-selected by the system. The subscriber ID is the same as the service on which the spoke is created. All other parameters are default values.

Redundant path selection

If Redundant Path Selection is enabled on a tunnel selection profile, a redundant path is created. Redundant Path Selection can only be enabled if Multi-Segment Tunnel Selection is also enabled. The selected redundant path does not use any of the same switching sites as the primary path. Redundant path selection is not supported when a termination point is selected on a spoke SDP binding. Table 61-2 describes the objects to which a tunnel selection profile with redundant path selection can be assigned, and the service tunnel configurations that result.

Table 61-2 Redundant path selection scenarios

Tunnel selection profile applied to...	Resulting redundant path configuration
Spoke SDP binding on a VLL service	This scenario applies to a VLL service with two terminating sites. One of the sites has a spoke SDP binding configured with Auto-Select Transport Tunnel enabled, and a tunnel selection profile with Multi-segment Tunnel Selection and Redundant Path Selection enabled. If a valid path is found between the two terminating sites, the spoke SDP bindings and switching sites for the redundant path are created. In this case, an endpoint and a return endpoint must be specified.
VLL service	This scenario applies to a VLL service with two terminating sites. The service is configured with Automatic SDP Binding/PBB Tunnel Creation enabled, and a tunnel selection profile with Multi-segment Tunnel Selection and Redundant Path Selection enabled. If a valid path is found between the two terminating sites, the spoke SDP bindings and switching sites for the redundant path are created. From a VLL Service, endpoints on the terminating sites that do not have SAPs or spokes are used for the auto-created spokes. If multiple endpoints exist on a terminating site, the endpoint without any SAPs is used. If multiple viable endpoints are available, an error is raised by the 5620 SAM and the operation fails. If there are no endpoints available, an endpoint is automatically created with default parameter values, with the following exceptions: • The Name parameter value is the endpoint Service ID. • The Description parameter value is auto-generated by the system.

SDP binding template handling

Multi-segment tunnel selection functionality will use SDP binding templates to create spoke SDP bindings in cases where a template is specified. SDP binding templates are handled using the following logic:

1 If an SDP binding template is specified on a tunnel selection profile, the template is used when creating the spoke SDP bindings.

2 If the site on which an SDP binding is being created has an associated site template, then the system attempts to find an SDP binding template within the site template. If an SDP binding template is found, it is used to auto-create the spoke SDP bindings. If two or more templates are found, the system creates a spoke SDP binding with default parameters. If no templates are found, the logic

described in item 3 applies.

3 If a service is associated with a template, then an attempt is made to find an SDP binding template within that template. If an SDP binding template is found, it is used to auto-create the spoke SDP bindings. If no templates are found, or two or more templates are found, then the system creates a spoke SDP binding with default parameters.

Service tunnel required bandwidth

Service tunnel bandwidth requirement can be specified as an additional constraint in the path search process. When required bandwidth is specified at the service or service site level, the selection of service tunnels is based on bandwidth availability. If all other tunnel selection criteria are equal, the tunnel with higher available bandwidth is selected.



Note 1 — Service tunnel required bandwidth functionality requires that the 5650 CPAM is licensed and configured against the current 5620 SAM install. Additionally, the Multi-Segment Tunnel Selection and Service Bandwidth Management system options must be enabled.

Note 2 — All physical links between service sites must be configured (either manually or through LLDP) before bandwidth can be allocated to service tunnels.

This functionality applies to RSVP tunnels on VLL, VPLS, and MVPLS services only. Bandwidth requirement criteria are specified at the service level, and are inherited by all associated service sites by default. Optionally, bandwidth requirement criteria can be specified on individual service sites. Bandwidth requirements are specified on the service or site configuration form, Bandwidth tab - Required Bandwidth sub-tab.

Bandwidth can be user-specified on a per-CoS basis, or it can be calculated automatically. When bandwidth values are calculated automatically, the calculation is based on the ingress CIR configurations, taking the sum of the bandwidths for the endpoints (SAPs) connected to each site. In the event that two sites with different bandwidth sums are connected by a service path, the lower of the two bandwidth sums is booked for the service path.

There are two options that determine how service bandwidth is booked in the network:

- For Epipe services only, the user has the option to enable bandwidth booking on both the active and redundant service paths (if a redundant path is available). Otherwise, only the active path is booked.
- For all VLL, VPLS, and MVPLS services, the user has the option to enable bandwidth booking on all operationally up LSP paths in use by the service. Otherwise, only the active path is booked.

Automatic PBB tunnel binding

This feature is applicable only to VLL Epipes and I-VPLS services using a PBB tunnel.



Note — This feature has limited availability. Contact your Alcatel-Lucent technical support representative for more information about the availability of this feature.

The configuration of the service CAC functionality allows you to manage bandwidth at the service level and at the link level, which in turn enables the 5620 SAM to automatically select the best tunnel based on the number of active links and on the amount of available bandwidth on the service. The 5620 SAM also considers the shortest available path when it allocates bandwidth.

Although the 5620 SAM can select tunnels automatically—see Automatic SDP (service tunnel) binding for services—if service CAC is not configured, bandwidth will not be considered by the 5620 SAM when selecting the tunnel.

Bandwidth availability for the tunnel is calculated at the service admission request time and is based on the links currently used by the tunnel forwarding path. The booking of reserved bandwidth by the service is done directly on the link and directly on the tunnel, for a bandwidth-reserved tunnel.

The link monitors the bandwidth used by all of the services using that link. Since the bandwidth reserved on each tunnel that is used by a service can be different, the link monitors bandwidth usage through the tunnels rather than through a service.

You can perform a system-wide audit to ensure that the bandwidth on each link is properly calculated. The audit visits all tunnels in the network and adjusts the available bandwidth in all links currently being used by the forwarding tunnel path. The adjustments are made based on total bandwidth requests per CoS for all EVPLs currently using the tunnels.

You can perform this audit by clicking on the CAC Audit button on the Manage Services form, or by choosing CAC Audit on the More Actions button. The audit also occurs automatically on system startup and when service CAC is switched from disabled to enabled. See “To configure service CAC to automatically bind PBB tunnels” in the *5620 SAM System Administrator Guide* for information about enabling and disabling service CAC.

Lightweight SAPs

SAPs that are associated with residential split horizon groups on VPLS sites are called lightweight SAPs. An RSHG uses dual-pass queue optimization and does not support downstream broadcast or multicast traffic. Lightweight SAPs have fewer internal configuration settings than regular SAPs. Therefore, you can create more lightweight SAPs on a NE. The SAP Lightweight property is automatically set at creation time, when the SAP is associated with an RSHG, and cannot be modified later.

Users can:

- assign SAPs to residential split horizon groups
- list lightweight SAPs using the Lightweight filter property

Note — To get the most recent state of a lightweight SAP, it is recommended that users perform a resynchronization by clicking on the Resync button in the SAP configuration form. If this button is not visible, click on the More Actions button and choose Resync.

61.2 5620 SAM and the triple play service delivery architecture

The TPSDA is based on three major components, as shown in Figure 61-6:

- broadband service aggregator
- broadband service router
- service and policy activation

Figure 61-6 TPSDA components

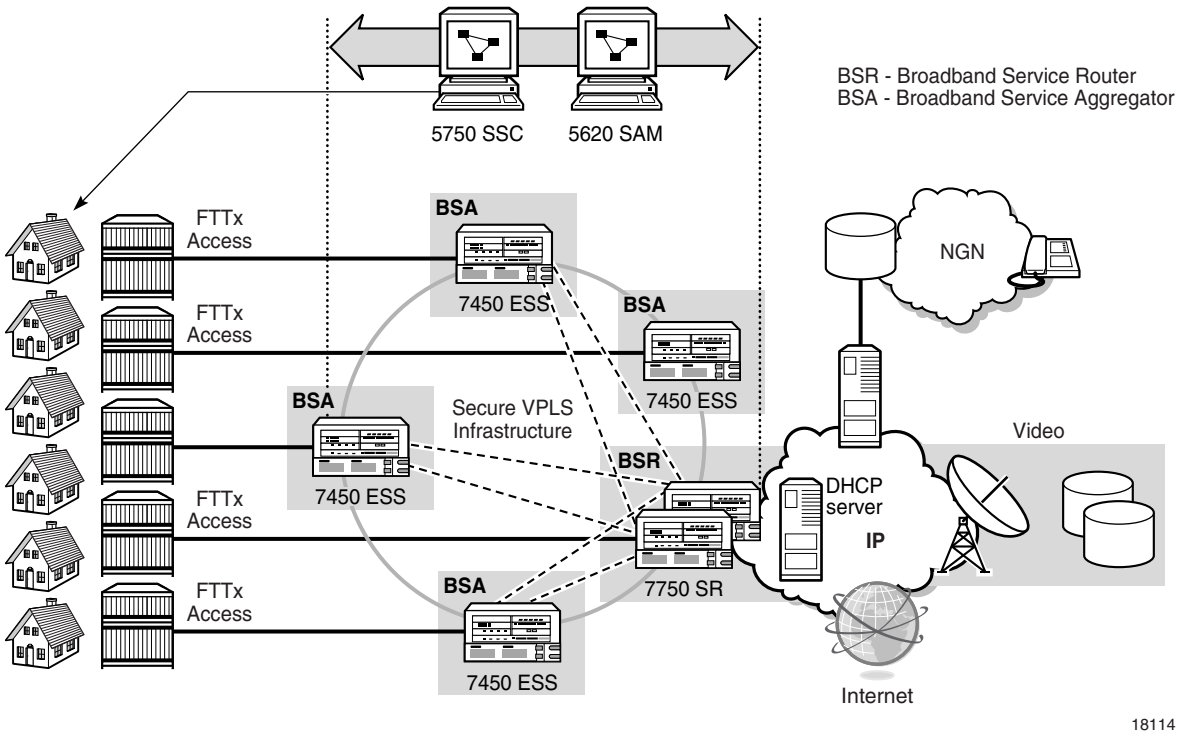


Table 61-3 lists the Alcatel-Lucent TPSDA product components.

Table 61-3 Product components of the TPSDA

Product	Role	Notes
5620 SAM	Provides network, service, and policy management across the TPSDA architecture, including a unified interface for element management and simple service activation and monitoring.	Create and configure QoS, filtering, and accounting templates that can then be reapplied to multiple L2 and L3 interfaces, and configure managed BSA and BSR devices to allow DHCP relay.
5750 SSC	Provides centralized control of host access services for triple play service delivery, for example, as a DHCP server to identify hosts and trigger service configuration or on-demand service profile changes made by the customer. Interworks with the 5620 SAM to enable per-customer QoS and bandwidth changes in the network.	Provide a customer self-service web portal and manage information that determines the levels of service allowed for an end user.
7750 SR	BSR	Support per-service and per-content type differentiation of QoS levels and supports distribution of multicast traffic.
7450 ESS	BSA	Aggregate traffic from DSLAMs and other FTTx access devices that are connected to end-user residential gateways.

DSLAMs or other access NEs are connected to Ethernet access ports on the broadband service aggregator. Typically, a single VLAN for each customer is set up between the access NE and the BSA. This a configuration enables the application of consistent per-customer policies, such as QoS, filtering, and accounting, to be applied on the BSA.

Scaling of traffic and services is done by dividing L2 and L3 functions between the BSA and the BSR. The BSA aggregates traffic over Gigabit Ethernet ports and performs per-customer service queueing, scheduling, accounting and filtering, as described later in this chapter. The BSR terminates L2 access and routes over IP/MPLS with support for all protocols, including multicasting. Time of day QoS policies can be applied using 5620 SAM policy management.

Interconnectivity between BSAs and BSRs is provided by VPLS. VPLS instances can be automatically established using hub-and-spoke or ring topologies. Both can be configured and sites added to the VPLS using the 5620 SAM. Regardless of the fiber plant layout, VPLS enables a full mesh between all sites that are receiving and distributing customer traffic in the TPSDA, ensuring efficient transport and protection from NE or fiber failures.

VPLS also provides mechanisms for traffic security, including residential split horizon groups in which direct user bridging is prohibited; ARP and broadcast suppression; DHCP-populated MAC and IP address filtering to prevent denial or service and theft of service using DHCP snooping, and RADIUS or TACACS+ authentication.

Service differentiation and QoS

This TPSDA approach provides a model based on call admission for video and VoIP, with the need to guarantee delay, jitter, and loss characteristics after the service connection is accepted. The architecture also meets the different QoS needs of HSI, namely per-user bandwidth controls, including shaping and policing functions that have little or no value for video and VoIP service delivery.

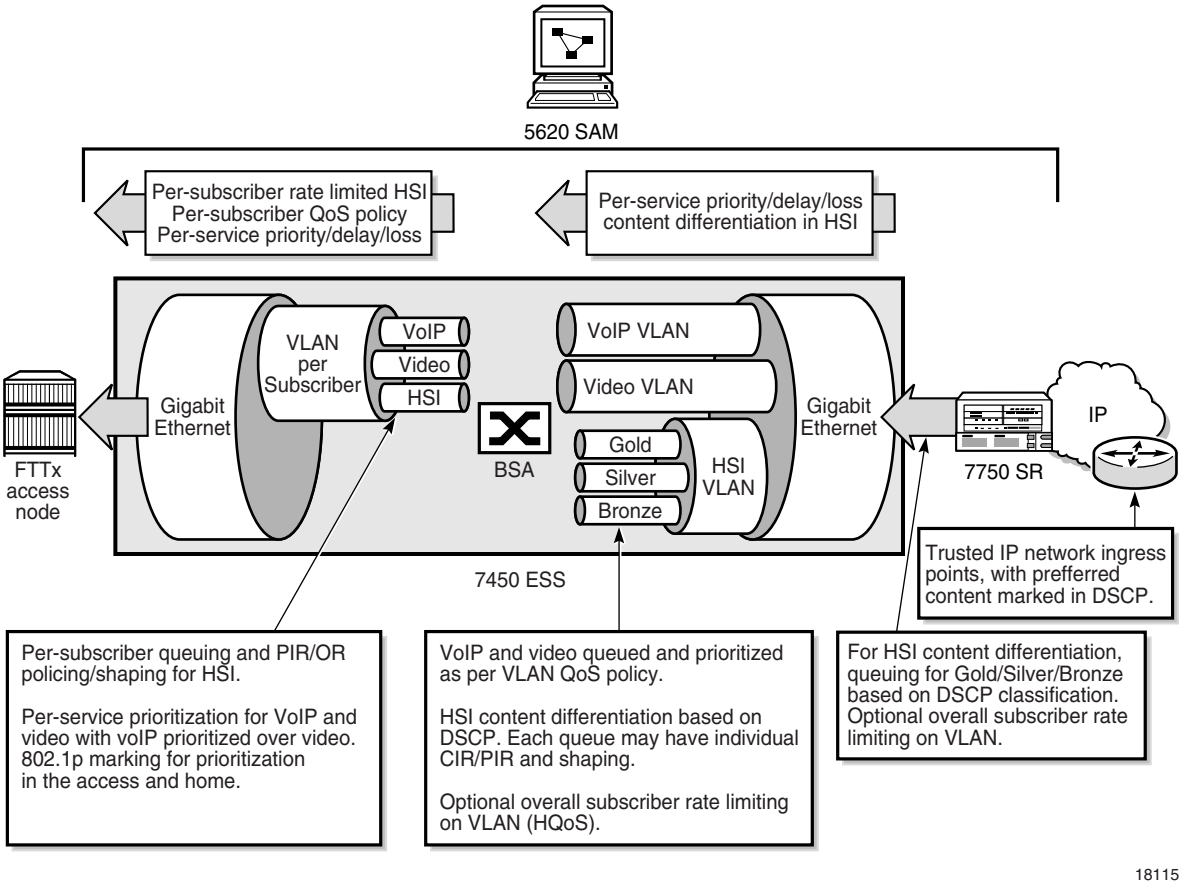
In conjunction with the architecture's support for content differentiation, this approach enables differentiated service pricing within high-priority data packages, also known as HSI. The distribution of QoS policy and enforcement across BSA and BSR allows the service provider to implement meaningful per-user service level controls. Sophisticated and granular QoS in the BSA allows the service provider to deliver truly differentiated IP services differentiation based on the user as well as on the content.

In the BSR to BSA downstream direction, IP services rely on IP layer classification of traffic from the network to queue traffic appropriately towards the BSA. Under extreme loading (only expected to occur under network fault conditions), lower priority data services and/or HSI traffic are compromised to protect video and voice traffic. Classification of HSI traffic based on source network address or IEEE 802.1p marking allows the QoS information to be propagated to upstream or downstream devices.

The BSR performs service distribution routing based on guarantees required to deliver the service and associated content, rather than on individual end users. The BSR only needs to classify content based on its forwarding class for a specific BSA to ensure that traffic for each service receives the appropriate treatment towards the BSA.

Figure 61-7 shows the downstream QoS configurations.

Figure 61-7 TPSDA downstream QoS configurations

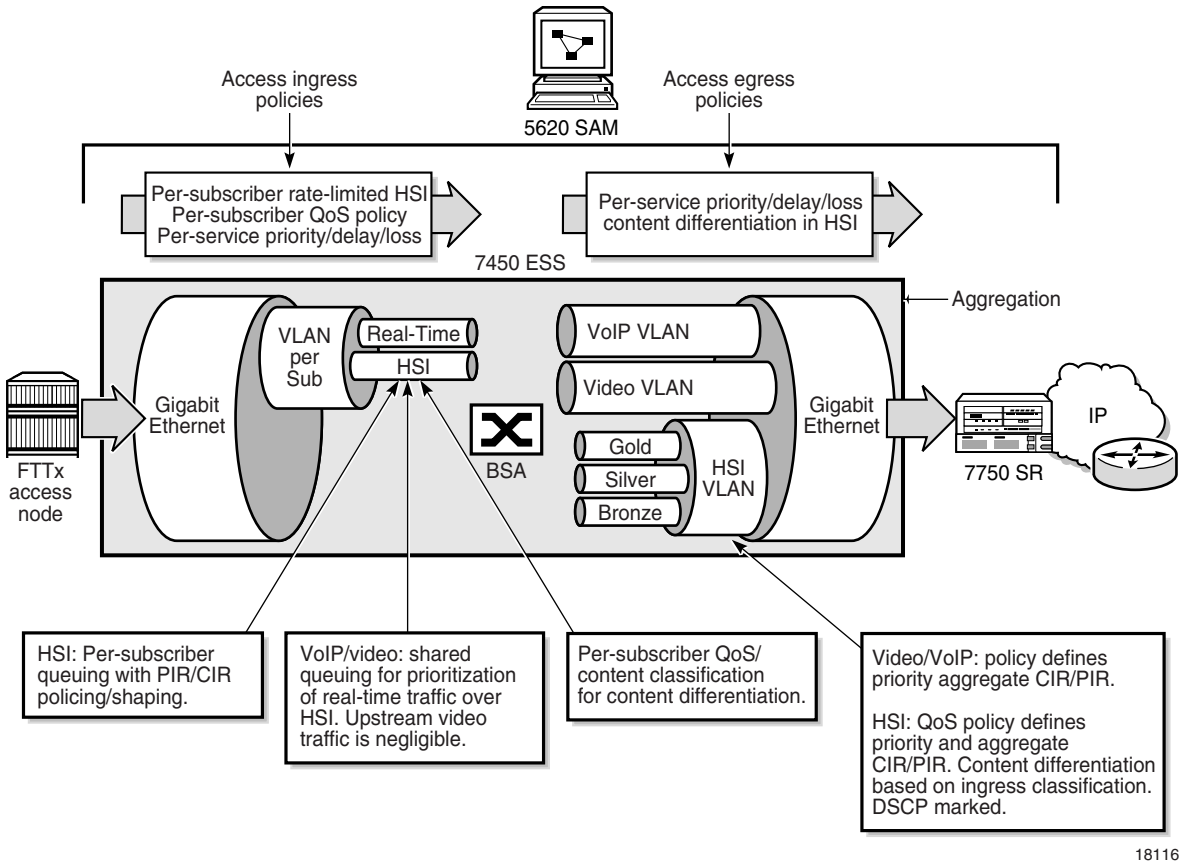


In the BSA-to-BSR upstream direction, traffic levels are substantially lower. Class-based queuing is used on the BSA network interface to ensure that video traffic is forwarded with minimal delay and that preferred data or HSI high-priority data traffic services receive better treatment than for best-effort Internet traffic. The IP edge device (BSR) therefore does not need to enforce per-user policies for hundreds of thousands of users. This function is distributed to the BSAs, and the per-user policies can be implemented on the interfaces directly facing the access NEs.

The BSA is capable of scheduling and queuing functions on a per-service, per-user basis, in addition to performing wire-speed packet classification and filtering based on both L2 and L3 interfaces. In addition to per-service rate limiting for Internet services, service traffic for each user can be rate-limited as an aggregate using a bundled service policy created using the 5620 SAM. These functions allow different users to receive different service levels independently and simultaneously.

Figure 61-8 shows the upstream QoS configurations.

Figure 61-8 TPSDA upstream QoS configurations



When a residential host device, such as a residential gateway or a set-top box in the customer's home, starts up, it requests network information, including the required IP address from a DHCP server. Figure 61-9 shows IP address assignment. See "5620 SAM and 5750 SSC integration" in the *5620 SAM Integration Guide* for information about using the 5750 SSC as a DHCP server. See Table 61-4 for more information about DHCP configuration options in the TPSDA.

Figure 61-9 DHCP IP address assignment in the TPSDA

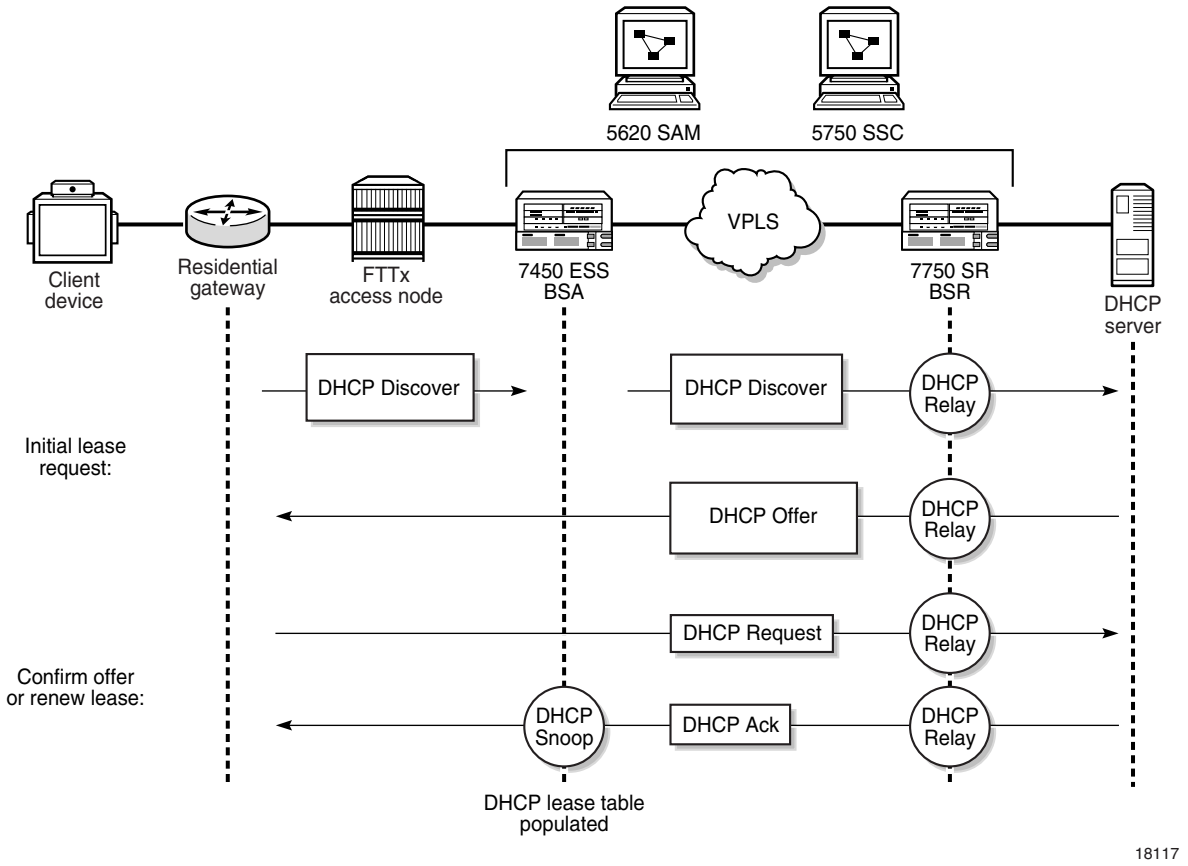


Table 61-4 lists the TPSDA features that you can configure using the 5620 SAM.

Table 61-4 TPSDA features

Feature and use	Notes	Reference
Split horizon groups		
For the TPSDA, there can be no user-to-user communication in the BSA; instead, all communication is done through the BSR. This residential bridging is done using split horizon groups, which ensures that traffic from different SAPs in the same service are not forwarded to other SAPs or spokes.	Traffic arriving on a spoke service tunnel or SAP within the split horizon group is not copied to other SAPs or spoke service tunnels. Traffic is copied to SAPs and spokes in other split horizon groups existing within the same service, such as a VPLS.	See chapter 68 for configuration of split horizon groups.
DHCP		

(1 of 3)

Feature and use	Notes	Reference
For the TPSDA, host devices, such as a residential gateway, SIP phone, or set-top box, use DHCP to obtain IP address and other network configuration information. The client device sends a DHCP discover message to request an IP address. The sequence of events is shown in Figure 61-9.	Information added to the DHCP discover requests may include information added by the FTTx access NE or the BSA, for example, the shelf, slot, port, VPI, VCI, or other identifier of the host. You can use the 5620 SAM to configure DHCP relay on the first IP interface in the upstream direction. The BSA or BSR relays the message to a DHCP server. The gateway (residential gateway) IP address indicates to the DHCP server the subnet an IP address should be allocated to for the host.	See the appropriate service configuration chapter, as DHCP, option 82, and DHCP relay are configured at the service level.
DHCP relay DHCP discover messages are broadcast packets that typically do not leave the IP subnet. DHCP relay agents intercept the requests and forward them as unicast messages to a DHCP server. DHCP request messages from subscriber hosts are usually sent from the FTTx access NE, with information appended to uniquely identify the residential gateway, either by MAC address of the residential gateway or by an option 82 string identifier that indicates the device, port type, rack, shelf, slot, port, and VLAN ID or VPI/VCI of the circuit connected to the residential gateway.	The DHCP relay agent sets the GIADDR in the packet to the IP address of the ingress interface (SAP). You must configure the BSA and BSR devices as DHCP relay agents when the DHCP requests are going to be forwarded to a DHCP server, or a 5750 SSC configured as a DHCP server. The maximum DHCP relay packet size is 1500 bytes.	See the appropriate L3 service (IES and VPRN) or L2 service (VPLS) configuration chapter. See the *5750 SSC Service Manager User Guide* and *5620 SAM Integration Guide* for more information about configuring the 5750 SSC as a DHCP relay agent.
DHCP lease state table The BSA maintains the identities of hosts that are allowed network access for each SAP on each service.	The lease state information is collected by snooping DHCP acknowledge messages on the SAP, using DHCP snooping. Entries in the DHCP lease state table remain valid for the duration of the IP address lease.	See chapter 16.
DHCP snooping The BSA can copy DHCP packets and inspect them to help secure the system. For example, if malicious user A sends an IP packet requesting a video stream intended for user B, return packets sent to user B could jam B's connection.	Use the 5620 SAM to configure DHCP snooping for the following purposes: • To insert Option 82 information when the system is not configured for DHCP relay by enabling DHCP snooping on the SAP closest to the host. • To build a DHCP lease state table by enabling DHCP snooping on the service tunnel nearest the network egress and on the SAP closest to the host. • To efficiently associate dynamic hosts with subscriber instances and associated network resources in a triple play service configuration	See the appropriate service chapters for configuration of the lease populate and snooping parameters. See chapter 65 for information about using DHCP snooping for subscriber identification purposes.

(2 of 3)

Feature and use	Notes	Reference
Option 82 The DHCP relay option allows managed devices to append information to the DHCP request that identifies where the DHCP request originated. You can also independently insert Option 82 information when DHCP snooping is enabled on a VPLS SAP. The Option 82 information can be: • The DHCP Option 82 string circuit ID value associated with the 7330 ISAM FTTN, or other ISAM family of NEs in the form ssc(*SSL-7330-1 atm 1/1/04/06:8.35*). The *device port_type rack/shelf/slot/port*:*VPI:VCI* identifier on the 7330 ISAM FTTN indicates that this is the connection configured for residential use, which is connected to the user's residential gateway. • The DHCP Option 82 string remote ID value associated with the 7330 ISAM FTTN, or other ISAM family of NEs in the form ssc(*remote ID*).	Using Option 82, you can identify: • the circuit ID (service tunnel binding) that is unique to the device relaying the circuit • the remote ID (MAC address) of the host at the far end of the circuit • the subscriber to which a host belongs for the purpose of assigning network resources The maximum DHCP relay packet size is 1500 bytes. If adding Option 82 information to the packet causes the packet to exceed 1500 bytes, the DHCP relay request is forwarded without including the Option 82 information.	See the appropriate service configuration chapter. For DHCP option 82 information inserted because of 5750 SSC DHCP server authentication, see the *5620 SAM Integration Guide*. For DHCP option 82 information inserted to identify subscribers, see chapter 65.

(3 of 3)

BTV multicast

This section describes how the 5620 SAM can be used to configure and manage the delivery of BTV multicast traffic streams. See section 61.3 for examples.

Optimizing for broadcast TV means implementing multicast packet replication throughout the network. Multicasting improves the efficiency of the network by reducing the bandwidth and fiber needed to deliver broadcast channels to the end user. A multicasting device can receive a single copy of a broadcast channel and replicate it to any downstream devices that require it, thus substantially reducing the required network resources. This efficiency becomes increasingly important closer to the end user.

Multicast routing overview

Multicast routers direct traffic to several receivers without incurring any additional overhead for the source router or the receivers. In contrast, unicast networks can suffer from increased bandwidth requirements as the number of receivers increases.

In multicast routing, receivers query the source router to request a specific data stream. The multicast group is not restricted by physical location, so long as the hosts can be reached through the Internet. Routers in the network must use IGMP to send and receive multicast data streams.

A multicast-enabled device, such as a switch or router, distributes a data stream to multiple receivers. Multicast packets are replicated in the network by routers that are enabled with PIM, which results in the efficient delivery of data to multiple receivers using less bandwidth.

1 A switch or router distributes a data stream to multiple receivers, such as multicast-enabled PE switches or routers.

2 The multicast-enabled switch or router replicates the data stream, when required, and transmits a copy to each downstream switch or router in the multicast tree.

3 Each client receives the data stream it has subscribed to from the downstream switch or router.

The NEs involved in delivering BTV multicast streams are first preconfigured through CLI for discovery and management by 5620 SAM. After discovery, routing protocols are applied to the NEs using 5620 SAM. Routing, QoS, and network queue policies are then created. On some devices, multicast package and ACL filter policies are created. These policies are applied to NEs during service creation through 5620 SAM.

Content delivery

BTV source traffic consists of one IP multicast stream per broadcast channel. As a multicast stream enters the core network, it is directed by PIM to the RP, which replicates the multicast traffic to all DRs that have requested the specific multicast stream. DRs distribute the multicast stream directly to set-top receivers or through an M-VPLS to BTV VLAN rings to which customer set-top receivers are connected. Multicast streams are forwarded only to those set-top receivers that have requested them through IGMP and are entitled to them as subscriber hosts.

Content management

Multicast package policies on some devices define the available multicast addresses (BTV channels) for end users in a BTV network. Typically, a root package policy which includes all BTV channels associated with a 5620 SAM customer service is created. Subsets of the root policy are then created as BTV content packages to which end customers can subscribe. ACL filter policies on CE devices ensure that only the channels to which an end customer has subscribed are delivered to the customer set-top receiver.

PIM

PIM uses RPF to correctly forward multicast packets down a distribution tree, using the independent multicast and unicast routing tables created by the 7450 ESS in mixed mode or the 7750 SR. The unicast routing table is populated by the unicast routing protocols, such as OSPF, BGP, IS-IS, or static routes, which can also be configured to submit routes to the multicast routing table.

Depending on the configuration of the PIM routing instance, RPF can use the unicast routing table, the multicast table populated by the unicast routing protocols, or both to determine the upstream sources of multicast streams. PIM forwards a multicast packet only if it is received on an upstream interface that is associated with a source address of an upstream router. This RPF check assures that there are no loops in the distribution tree.

PIM uses a multicast domain to group receiver hosts on a router called the rendezvous point (RP). A bootstrap router (BSR) elects an RP from available candidates. The BSR manages RP information, disseminates it to all PIM routers in the multicast domain, and elects a new RP in the case of RP unavailability.

A receiver host becomes a member of a multicast domain by sending an IGMP join request for a multicast stream to a PIM designated router (DR). If the router does not currently receive the multicast stream, PIM updates the DR routing table with the receiver host IP address and requests the multicast stream from the RP. The RP adds the router to the distribution tree. Packets sent to the multicast IP address are propagated down the distribution tree to the receiver host. DRs use the RP as the source for a multicast stream unless a source with a lower path cost is available.

PIM stops sending a multicast stream to a router when it determines that there are no active receiver hosts for the multicast stream in that branch of the distribution tree.

MVR on VPLS

PIM is not supported on 7450 ESSs. When receiver hosts are connected to a PIM DR by way of a 7450 ESS, MVR must be configured on the switch. MVR allows multicast traffic to be forwarded downstream from the DR to the receiver host over an MVR VPLS.

IGMP

IGMP is a multicast protocol which service providers can use to establish multicast group memberships on a LAN. Within the LAN, end users use IGMP to communicate with a local multicast router, which then uses PIM to distribute the IGMP messages to other local and remote multicast routers. Multicast routers send regular membership queries to IGMP hosts which respond with membership reports. Multicast routers can use these reports to determine which hosts are interested in receiving particular multicast messages.

IGMP operates above the network layer on IPv4 networks.

MLD and MLD-snooping

The Multicast Listener Discovery protocol is essentially the IPv6 version of IGMP. It is used by IPv6 routers to discover the presence of multicast listeners (that is, NEs that wish to receive multicast packets) on their directly attached links, and to discover specifically which multicast addresses are of interest to those neighboring NEs.

MLD version 2 (MLDv2) is designed to be interoperable with MLD version 1 (MLDv1). MLDv2 adds the ability for a NE to report interest in listening to packets with a specific multicast address only from specific source addresses or from all sources except for specific source addresses.

Most 5620 SAM NEs support MLD-snooping but not MLD. The 7450 ESS, 7710 SR, 7750 SR, and 7950 XRS routers allow the enabling of MLD snooping for VPLS services. All variants of the 7705 SAR support MLD but not MLD-snooping.

61.3 BTV multicast configuration examples

Figure 61-10 shows a simple BTV network and three methods of content delivery, examples A, B, and C. The sequence of specific configuration steps for each example follows general device, network and multicast configuration information common to all examples.



Note — In the examples on the following pages, references to "IGMP-snooping" may generally be read as "IGMP- or MLD-snooping", provided the routers employed in the configurations support the MLD protocol.

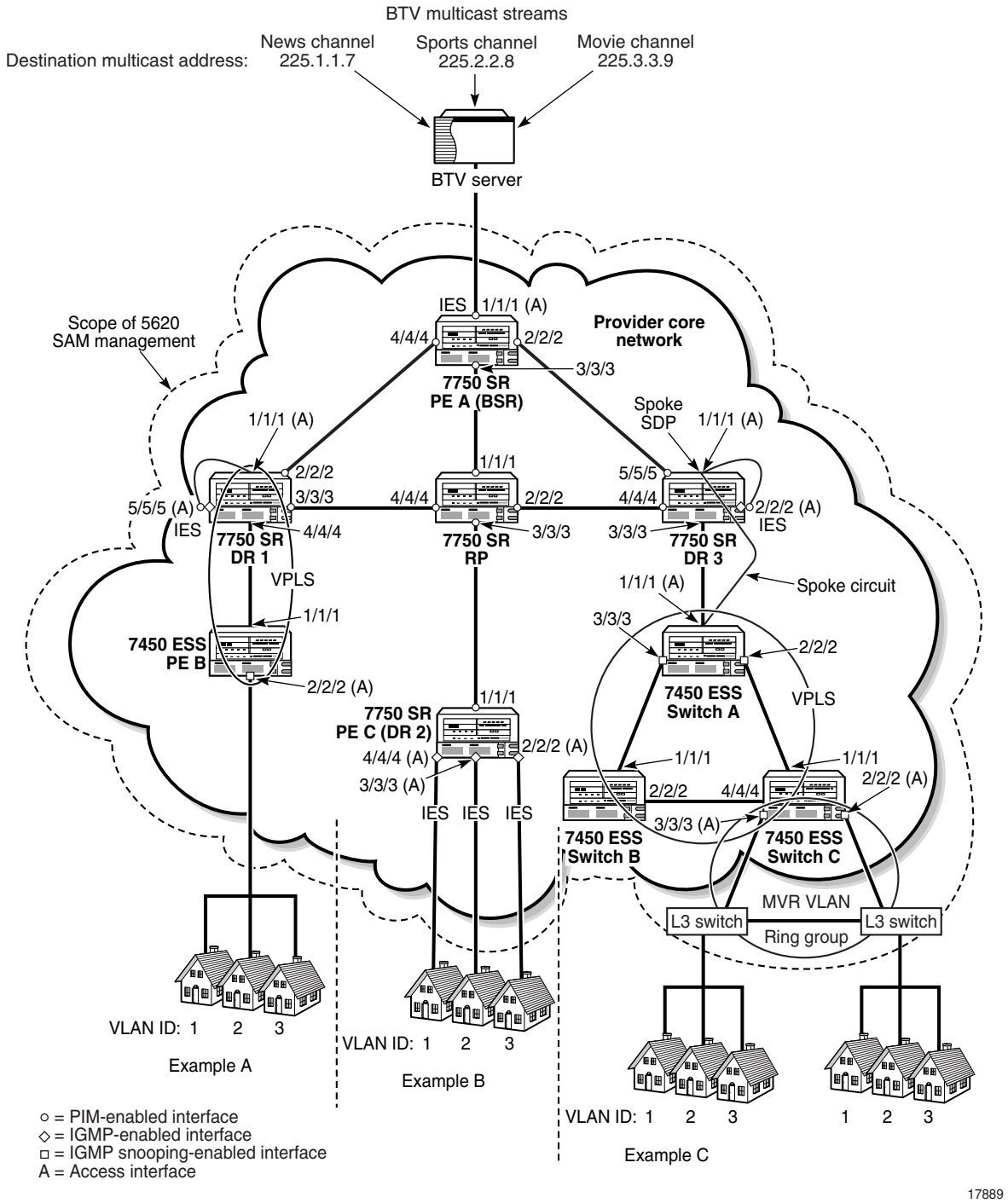
Device preconfiguration

A network device requires CLI preconfiguration before it can be managed by the 5620 SAM. The primary CLI preconfiguration actions for a device are:

- Assigning a system ID to the device
- Enabling and configuring SNMP on the device
- Enabling Telnet access on the device

See chapter 1 and the specific device documentation for more information about enabling device functionality before using the 5620 SAM.

Figure 61-10 BTV multicast delivery examples



After CLI preconfiguration, further actions are required:

- Discover devices, including mediation configuration with CLI user names and passwords.
- Use 5620 SAM to set the discovered device in a managed state.

See chapter 10 for more information about device discovery and management using 5620 SAM.

Network preconfiguration

The core network shown in Figure 61-10 represents a fully meshed group of devices. For simplicity, only the devices relevant to the BTV multicast examples are shown. Network preconfiguration consists of the following sequence of actions:

1 Configure network devices for in-band or out-of-band management. See chapter 9 for more information.

2 Configure a system interface on each device to serve as the identifier for the device. See chapter 22 for more information.

3 Configure network interfaces on each router to establish a full mesh of interconnectivity between devices. In Figure 61-10 the interfaces to be configured are PE A, ports 1/1/1, 2/2/2, 3/3/3, and 4/4/4; DR 1, port 2/2/2; RP, ports 1/1/1, 2/2/2, and 4/4/4; and DR 3, ports 1/1/1 and 4/4/4. See chapter 22 for more information.

4 Cable the network-interface ports between routers in the core network to establish the physical connectivity shown in Figure 61-10.

5 Use CLI ping commands to check IP connectivity between devices. See the device documentation for more information.

6 Enable IGPs such as RIP, OSPF, or IS-IS on devices according to network size and complexity. See chapter 23 for information about enabling routing protocols.

7 Enable an inter-AS routing protocol such as BGP or OSPF to PE routers, if required. See chapter 23 for more information.

8 Create routing policies as required. Create one multicast group for each BTV multicast destination address during policy creation. See chapter 22 for more information.

9 Configure routing protocols and apply routing policies as required. See chapter 23 for more information.

10 Configure LDP and MPLS, if required. See chapter 23 for information about configuring LDP. See chapter 25 for information about configuring MPLS.

- Enable MPLS and LDP on the routing instance of each device that is participating in the MPLS network.
- Assign a Layer 3 interface to the MPLS instance on each MPLS-enabled device.
- Create a mesh of MPLS paths.
- Create a mesh of LSPs.
- Use the 5620 SAM to create MPLS administrative groups, and assign the groups to MPLS interfaces and LSP paths as required.

Multicast configuration common to all examples

The network connections shown between PE A and DR 1 and between PE A and DR 3 represent redundant multicast routes used by PIM in the event of an RP failure. PIM dynamically adjusts to BSR or RP failure by electing a replacement BSR or RP or by using a previously defined backup BSR or RP. PIM chooses the most appropriate source for a multicast stream based on path cost and source availability and bypasses the RP if a better source for a multicast stream is found.

For simplicity, Figure 61-10 does not show routes to PE C (DR 2) from DR 1 or DR 3. As shown, PE C (DR 2) is isolated from multicast traffic in the event of RP failure.

Network multicast configuration common to all three examples involves the following sequence of actions:

1 Enable IGMP on routers DR 1, PE C (DR 2), and DR 3. See Procedure 23-45 for more information.

2 Configure IGMP on routers DR 1, PE C (DR 2), and DR 3. See Procedure 23-46 for more information.

3 Enable PIM on routers PE A, RP, DR 1, PE C (DR 2), and DR 3. See Procedure 23-39 for more information.

4 Configure PIM on routers PE A, RP, DR 1, PE C (DR 2), and DR 3. See Procedure 23-40 for more information.

- Specify PE A as the candidate bootstrap router.
- Specify RP as the candidate rendezvous point. You can also specify it as a static RP for a multicast domain, if there are multiple BTV domains, and configure a second router as a redundant RP.
- Specify IES as the Apply to parameter value on routers PE A, DR 1, PE C (DR 2), and DR 3.

5 Create PIM interfaces at PE A, ports 1/1/1, 2/2/2, 3/3/3, and 4/4/4; RP, ports 1/1/1, 2/2/2, 3/3/3 and 4/4/4; DR 1, ports 2/2/2 and 3/3/3; DR 2, port 1/1/1 and DR 3, ports 4/4/4 and 5/5/5. See Procedure 23-43 for more information.

6 Create QoS, scheduling, and accounting policies for the ingress BTV traffic. See chapter 42 for more information.

7 Create an IES from PE A, port 1/1/1, to the BTV multicast provider's network. See Procedures 70-1 and 70-3 for more information.

- Enable PIM on the IES SAP during IES creation.

Example A configuration

In Example A, IGMP join requests from residential hosts ingress a VPLS SDP. IGMP snooping on the VPLS registers the join requests on the local switch. The switch sends the requests over the VPLS, which is physically cross-connected to an IGMP- and PIM-enabled IES SAP on the DR. PIM on the DR requests the desired multicast stream, if not present, from the RP. The requested stream then traverses the VPLS and is sent to end users.

1 Configure PE B, port 1/1/1 and DR 1, port 4/4/4 as network ports. See Procedure 16-1 for more information.

2 Configure PE B, port 2/2/2 and DR 1, port 1/1/1 as access ports. See Procedure 16-1 for more information.

3 Cable DR 1, port 3/3/3, and PE B, port 1/1/1 to establish physical connectivity.

4 Configure DR 1, port 5/5/5 as an access port. See Procedure 16-1 for more information.

5 Create an IES on DR 1, port 5/5/5. See Procedures 70-1 and 70-3 for more information.

- Enable IGMP on the IES SAP during IES creation.
- Enable PIM on the IES SAP during IES creation.

6 Connect a cable between ports 1/1/1 and 5/5/5 on DR 1 as a service cross connect.

7 Create QoS, scheduling, filter, and accounting policies to apply to egress BTV traffic during service creation. See chapter 42 for information about policy creation.

8 Create a distributed VPLS with endpoints at PE B, port 2/2/2 and DR 1, port 1/1/1. See Procedures 68-1 and 68-7 for more information.

- Enable IGMP snooping on the VPLS SDP at PE B, port 2/2/2.
- Apply previously defined QoS, scheduling, filter, and accounting policies to the VPLS SDP at PE B, port 2/2/2.

Example B configuration

In Example B, an IGMP join request ingresses an IES SAP on the DR. PIM on the DR requests the desired multicast stream, if not present, from the RP. The requested stream is then delivered over an IES to an end user.

1 Configure PE C (DR 2), ports 2/2/2, 3/3/3, and 4/4/4 as access ports. See Procedure 16-1 for more information.

2 Create QoS, scheduling, filter, and accounting policies to apply to egress BTV traffic during IES creation. See chapter 42 for information about policy creation.

3 Create IES services on PE C (DR 2), ports 2/2/2, 3/3/3, and 4/4/4 that terminate on the CE set-top devices. See Procedure 70-1 for more information.

- Enable IGMP on each IES SAP during IES creation.
- Apply previously defined QoS, scheduling, filter, and accounting policies to each IES, as required.

Example C configuration

In Example C, IGMP join requests from residential hosts pass over an MVR VLAN to an VPLS. IGMP snooping on the VPLS registers the join requests on the local switch, which passes them over the VPLS to a spoke SDP on the DR. The spoke SDP's port is physically cross-connected to an IGMP- and PIM-enabled IES SAP on the DR. PIM on the DR requests the desired multicast stream, if not present, from the RP, then sends the stream over the VPLS and MVR VLAN to the end users.

1 Create a BTV MVR VLAN of L3 switches in a ring group with endpoints on Switch A, ports 2/2/2 and 3/3/3. See section 66.3 and Procedure 66-3 for more information. For redundancy, the MVR VLAN can be configured with endpoints on different switches. A VLL between the two switches acts as an unbreakable connection.

2 Enable and configure IGMP snooping on the bridge instances for the L3 switches included in the MVR VLAN.

3 Create QoS, scheduling, filter, and accounting policies to apply to egress BTV traffic during service creation. See chapter 42 for information about policy creation.

4 Configure the following as network ports:

- Switch A, ports 1/1/1, 2/2/2, and 3/3/3
- Switch B, ports 1/1/1 and 2/2/2
- Switch C, ports 1/1/1, 2/2/2, 3/3/3 and 4/4/4

See Procedure 16-1 for more information.

5 Create a distributed VPLS consisting of Switch A, Switch B, and Switch C. See Procedures 68-1 and 68-7 for more information.

- Apply previously defined QoS, scheduling, filter, and accounting policies to the VPLS SDPs.
- Enable and configure IGMP snooping on the VPLS SDPs that are part of the MVR VLAN.
- Ensure that the encapsulation value of the VPLS SDPs that are part of the MVR VLAN matches the MVR VLAN ID.
- Create a split horizon group during VPLS creation to allow later addition of a spoke circuit to the VPLS.
- Configure STP on the VPLS, as required.

6 Configure DR 3, port 2/2/2 as an access port. See Procedure 16-1 for more information.

7 Create an IES on DR 3, port 2/2/2. See Procedures 70-1 and 70-3 for more information.

- Enable IGMP on the IES SAP during IES creation.
- Enable PIM on the IES SAP during IES creation.

8 Connect a cable between ports 1/1/1 and 2/2/2 on DR 3 as a service cross connect.

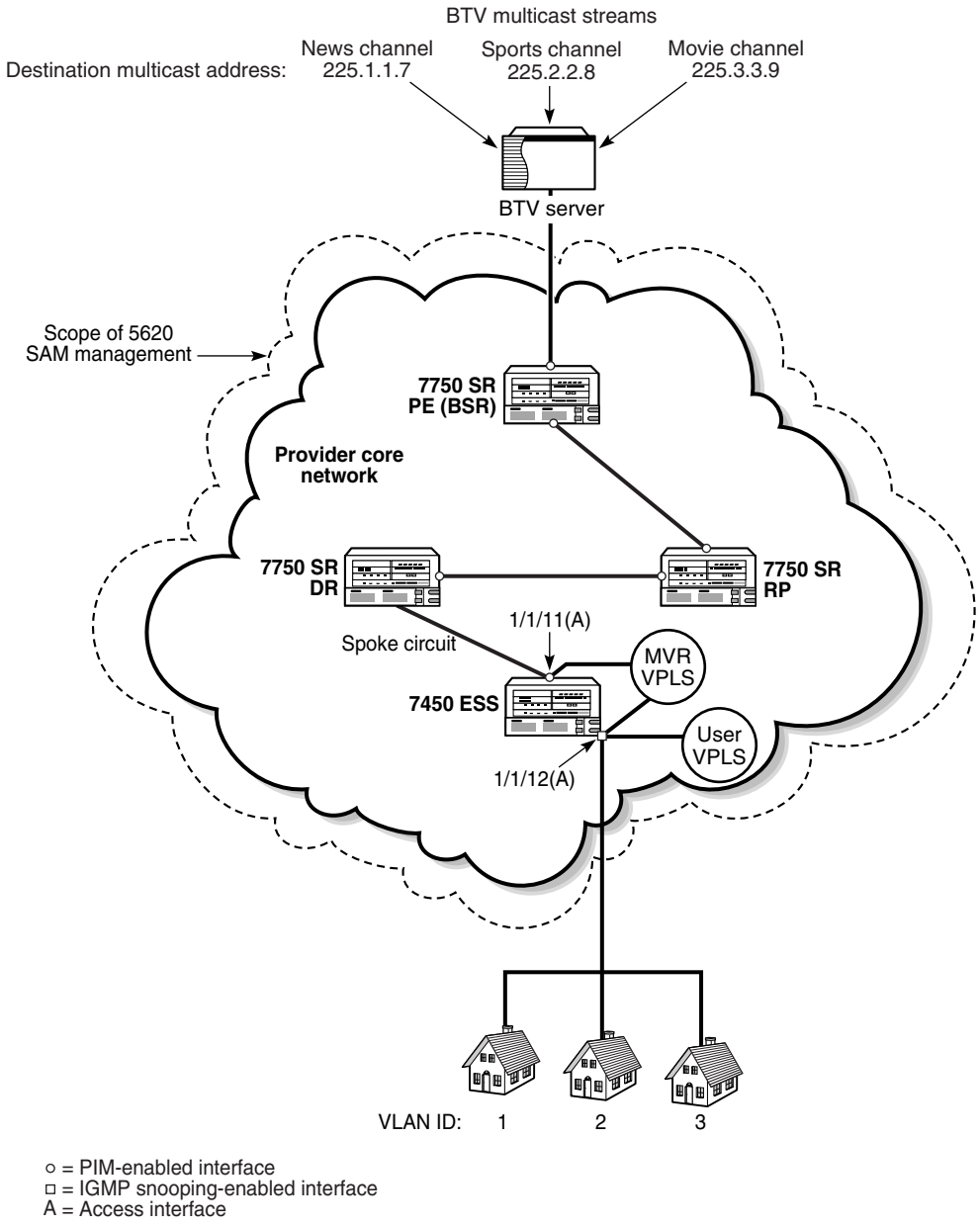
9 Create a VPLS spoke SDP at DR 3, port 1/1/1. See Procedure 68-58 for more information.

Example D configuration

Figure 61-11 shows an example of BTV multicast delivery using MVR on VPLS.

See Figure 61-10, and sections "Network preconfiguration" and "Multicast configuration common to all examples" for common network configuration information.

Figure 61-11 BTV multicast delivery using MVR on VPLS example



In Example D, IGMP join requests from residential hosts are sent to a user VPLS on the 7450 ESS. IGMP snooping on the user VPLS registers the join requests on the switch, which sends them to the 7750 SR DR. PIM on the DR requests the desired multicast stream, if not present, from the RP, then sends the stream over the MVR VPLS to the user VPLS, from which the multicast stream is sent to the end users.

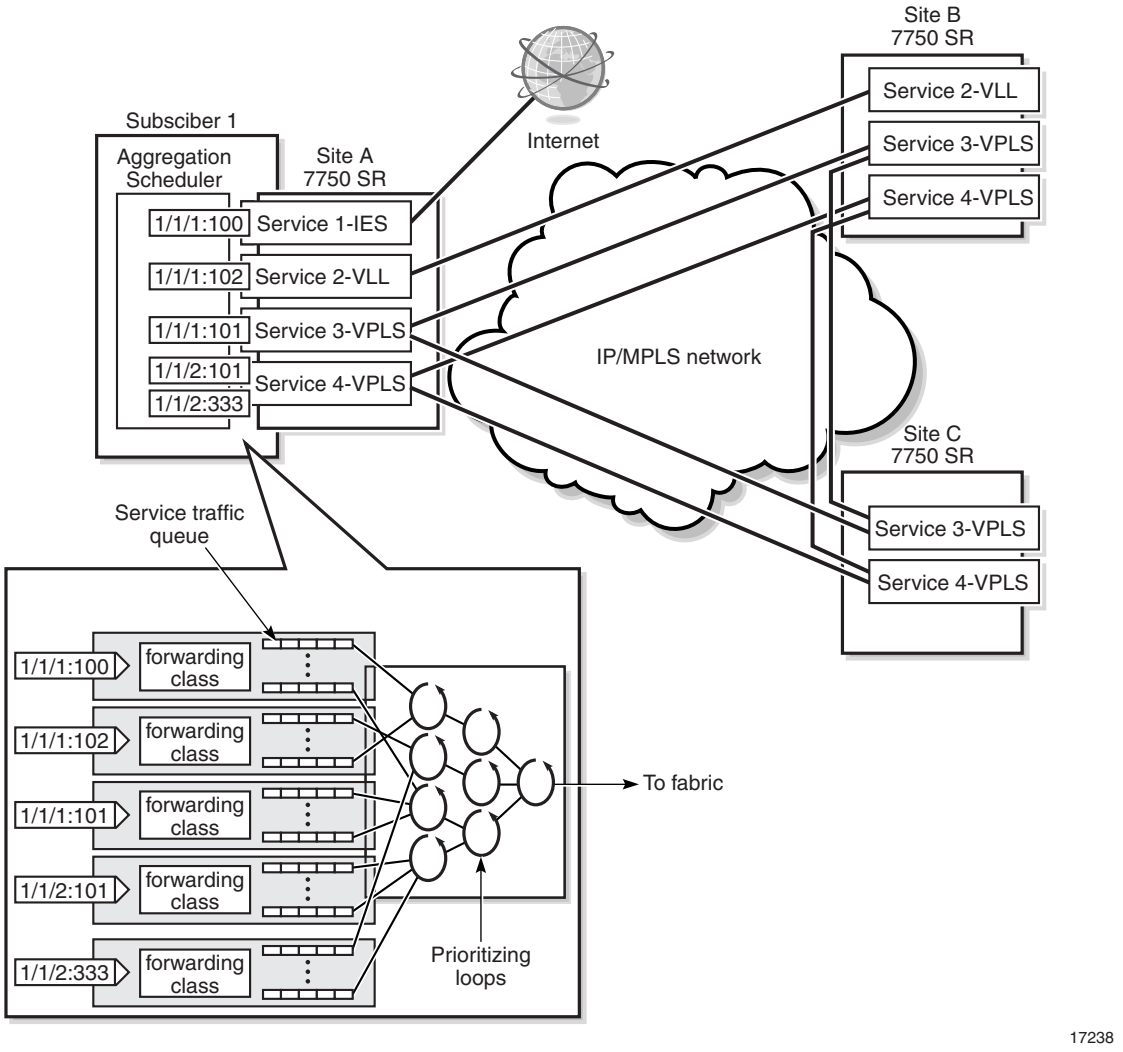
1 Create a multicast package policy to apply to the 7450 ESS that belongs to the MVR VPLS. See chapter 45 for more information.

2 Configure the following ports as access ports. See Procedure 16-1 for more information.
   - 7450 ESS, port 1/1/11
   - 7450 ESS, port 1/1/12
3 Create an MVR VPLS on the 7450 ESS with SAPs 1/1/11 and 1/1/12. Apply the previously defined multicast package policy to the MVR VPLS.
4 Create a user VPLS on SAP 1/1/12 of the 7450 ESS.
   - Associate the user VPLS with the previously created MVR VPLS to identify the MVR VPLS as the source of the multicast traffic.
   - Enable and configure IGMP snooping on the site.
5 Create a spoke circuit between the 7450 ESS (endpoint 1/1/11) and the 7750 SR DR.

61.4 Sample network configuration using QoS

Figure 61-12 shows an example of a service configuration using QoS.

Figure 61-12 Example of a service configuration using QoS



In this configuration, the following services are provisioned:

- Service 1: IES for Internet access, which requires a CIR of 10 Mb/s and a PIR of 100 Mb/s
- Service 2: VLL service for FTP connectivity between Site A and Site B, which requires a CIR of 10 Mb/s and a PIR of 20 Mb/s
- Service 3: VPLS for video-conference service over sites A, B, and C, which requires a CIR of 20 Mb/s and a PIR of 50 Mb/s
- Service 4: VPLS for voice traffic, which requires a CIR of 10 Mb/s and a PIR of 20 Mb/s

The cumulative rate at site A needs to be limited to 70 Mb/s.

The following high-level steps are required to create the Figure 61-12 configuration with rate limiting using QoS at Site A. Similar steps are required to configure QoS for Subscriber 1 on Sites B and C:

1 Configure a scheduler policy.

2 Create Subscriber 1.

3 Create the aggregation scheduler for Subscriber 1 on site A and assign ingress and egress scheduler policies to the aggregation scheduler.

4 Create IES, VLL, and VPLS for Subscriber 1.

- Specify sites for the services.
- Specify access interfaces for the sites.
- Specify the aggregation scheduler policy for the access interfaces.
- Bind the services to tunnels for transport through the IP/MPLS network.

Access interfaces 1/1/1:100, 1/1/1:101, 1/1/1:102, and 1/1/2:101 participate in the aggregation scheduler and are usually rate limited by the rate specified in the scheduler policy.

Access interface 1/1/2:333 does not participate in scheduler policy; rate limiting is specified by the queue values.

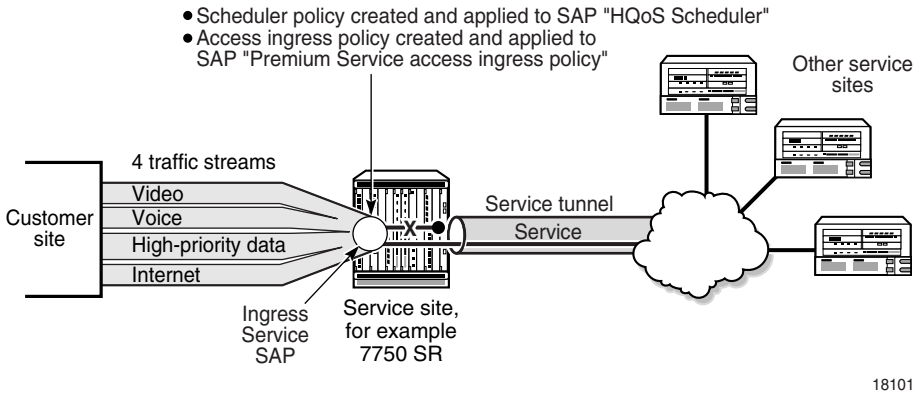
If one of the access interfaces does not participate in the scheduler aggregator, it may be managed by a separate scheduler policy.

61.5 Sample SAP QoS configuration

You can use 5620 SAM to configure and enforce traffic rate limiting, based on the priority of the traffic entering the ingress SAP of a service. This configuration limits bandwidth, to ensure that SLAs are met and higher priority traffic is processed first.

Figure 61-13 shows traffic of different priorities from a customer site to an ingress SAP.

Figure 61-13 Example showing ingress traffic to a service SAP



Based on the example, use the 5620 SAM client GUI to perform the following actions:

- Configure a parent scheduler that handles scheduling for a child scheduler.

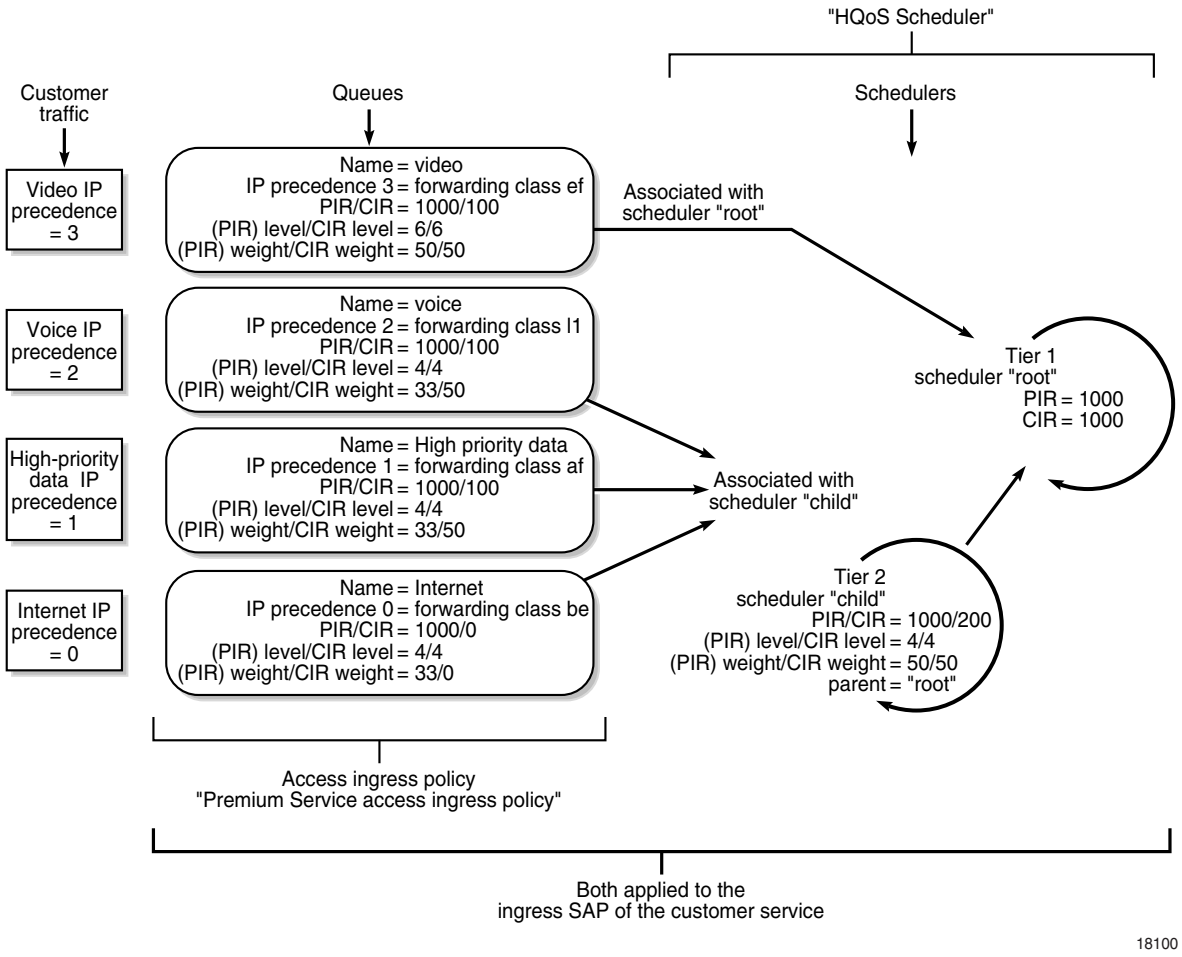


Note — You do not have to configure a parent tier 1 scheduler for a child tier 2 scheduler. You can create a tier 2 scheduler on its own, with no parent. This example is meant to show hierarchical QoS.

  - Add a root tier 1 scheduler
  - Add one child tier 2 scheduler with the root scheduler as a parent
- Create an access ingress policy named Premium service access ingress policy.
  - Create 4 queues within the access ingress policy, one for each type of traffic from the customer site.
  - Associate each queue with a forwarding class
  - Classify the incoming customer site traffic to a forwarding class. For this sample, IP precedence is used to classify traffic. You could classify traffic other ways, for example, based on filters for IP address or DSCP marking.
  - Associate each queue with the appropriate scheduler.
- Apply the schedulers and access ingress policy to the appropriate L2 or L3 interface for the customer service, for example, a VPLS L2 interface.

Figure 61-14 shows how traffic is handled based on the ingress access policy and scheduler queue handling applied to the ingress service SAP.

Figure 61-14 Traffic handling based on ingress access policy and scheduler queue



In this sample:

- higher-priority video traffic, with IP precedence bit 3 set, goes into queue 4 with a PIR of 1000 Kb/s and a CIR of 100 Kb/s. This traffic is handled by the tier 1 scheduler. The levels and weights associated with the video queue (forwarding class of ef, level of 6, PIR/CIR weights of 50/50) ensure this traffic gets all required bandwidth.
- all other traffic goes into its appropriate queues, based on the mapping of the IP precedence bit with the forwarding class.
- The voice, high-priority data, and Internet queues are serviced by the tier 2 scheduler.
- Because the voice and high-priority data queues have higher PIR/CIR weight than the Internet queue, when there is contention for bandwidth, the voice and high-priority data queues are processed first.

Preconfiguration

1 Before you begin, you must have:

- the service ingress SAP configured as access
- all necessary cabling and network routing protocol configurations complete to handle routing packets to and from the CPE equipment

Configuration

2 Choose Policies→QoS→SROS QoS→Scheduler→Scheduler from the 5620 SAM main menu. The manage scheduler policies form opens.

3 Click on the Create button. The scheduler policy create form opens.

4 Configure the parameters. Set the displayed name to High QoS.

5 Click on the Schedulers tab.

6 Click on the Create button. The scheduler entry form opens.

7 Create a root, tier 1 scheduler entry,

i Configure the parameters.

- Displayed name to root
- tier to 1
- Summed CIR to false
- PIR (kbps) to 1000
- CIR (kbps) to 1000

ii Click on the OK button. The root scheduler appears in the list of scheduler entries.

8 Create a child, tier 2 scheduler entry.

i Click on the Create button.

ii Configure the parameters.

- Displayed name to child
- tier to 2
- Summed CIR to false
- PIR (kbps) to 1000
- CIR (kbps) to 200
- Parent scheduler to root, using the Select button to choose root from the list.
- Level (PIR level) to 4
- Weight (PIR weight) to 50
- CIR Level to 4
- CIR Weight to 50

iii Click on the OK button. The child scheduler appears in the list of scheduler entries.

9 Click on the Apply button.

10 Close the Scheduler form.

11 Choose Policies→QoS→SROS QoS→Access Ingress→Access Ingress from the 5620 SAM main menu. The Access Ingress Policies form opens.

12 Click on the Create button. The Access Ingress Policy, Global Policy [Create] form opens.

13 Configure the parameters. Set the displayed name to Premium service access ingress policy.

14 Click on the Queues tab. Create four queues. For this sample, default queue 1 is modified, and three new queues are added. The default multicast queue 11 is unchanged.

15 Select queue 1 from the list.

i Click on the Properties button. The queue 1 edit form opens.

ii Configure the parameters.

- Displayed Name to Internet
- Scheduler to child by using the Select button and choosing child from the list
- Level (PIR level) to 4
- CIR Level to 4
- Weight (PIR weight) to 33
- CIR Weight to 0

iii Click on the CIR/PIR tab.

iv Configure the parameters.

- Rate Type to kbps
- Policed to false
- deselect both MAX buttons
- Cir (kbps) to 0
- Pir (kbps) to 1000

v Click on the OK button.

16 Add queue 2.

i Click on the Create button. The queue create form opens.

ii Configure the parameters.

- ID to 2
- Displayed Name to High-priority traffic
- Scheduler to child by using the Select button and choosing child from the list
- Level (PIR level) to 4
- CIR Level to 4
- Weight (PIR weight) to 33
- CIR Weight to 50

iii Click on the CIR/PIR tab.

iv Configure the parameters.

- Rate Type to kbps
- Policed to false
- deselect both MAX buttons
- Cir (kbps) to 100
- Pir (kbps) to 1000

v Click on the OK button. The queue is added to the list.

17 Add queue 3.

i Click on the Create button. The queue create form opens.

ii Configure the parameters.

- ID to 3
- Displayed Name to Voice
- Scheduler to child by using the Select button and choosing child from the list
- Level (PIR level) to 4
- CIR Level to 4
- Weight (PIR weight) to 33
- CIR Weight to 50

iii Click on the CIR/PIR tab.

iv Configure the parameters.

- Rate Type to kbps
- Policed to false
- deselect both MAX buttons
- Cir (kbps) to 100
- Pir (kbps) to 1000

v Click on the OK button. The queue is added to the list.

18 Add queue 4.

i Click on the Create button. The queue create form opens.

ii Configure the parameters.

- ID to 4
- Displayed Name to Video
- Scheduler to root by using the Select button and choosing root from the list
- Level (PIR level) to 6
- CIR Level to 6
- Weight (PIR weight) to 50
- CIR Weight to 50

iii Click on the CIR/PIR tab.

iv Configure the parameters.

- Rate Type to kbps
- Policed to false
- deselect both MAX buttons
- Cir (kbps) to 100
- Pir (kbps) to 1000

v Click on the OK button. The queue is added to the list.

19 Click on the Apply button to save the changes. Confirm the action.

20 Associate each queue with a forwarding class.

i Click on the Forwarding Classes tab.

ii Click on the Create button. The forwarding class create form opens.

iii Configure the parameters.

- Forwarding class to be
- Queue ID to 1. This is the best-effort Internet traffic queue.

iv Click on the OK button. Confirm the action.

v Click on the Create button. The forwarding class create form opens.

vi Configure the parameters.

- Forwarding class to af
- Queue ID to 2. This is the high-priority data traffic queue.

vii Click on the OK button. Confirm the action.

viii Click on the Create button. The forwarding class create form opens.

ix Configure the parameters.

- Forwarding class to l1
- Queue ID to 3. This is the voice traffic queue.

x Click on the OK button. Confirm the action.

xi Click on the Create button. The forwarding class create form opens.

xii Configure the parameters.

- Forwarding class to ef
- Queue ID to 4. This is the highest priority, video traffic queue.

xiii Click on the OK button. Confirm the action.

21 Click on the Apply button. Confirm the action.

22 Associate the IP precedence bits of the incoming customer traffic with the forwarding class. The forwarding class is already associated with a queue. For this sample, IP precedence bits are used to associate different types of traffic with the forwarding class. You could classify traffic other ways, for example, based on filters for IP address or DSCP marking.

i Click on the Precedence tab.

ii Click on the Create button. The precedence create form opens.

iii Configure the parameters to associate IP precedence 0 (Internet traffic from the customer site) with forwarding class be (the be forwarding class is associated with queue 1)

- Precedence is 0
- Forwarding Class is be

iv Click on the OK button. Confirm the action. The association between precedence 0 and the be forwarding class is added to the list.

v Click on the Create button. The precedence create form opens.

vi Configure the parameters to associate IP precedence 1 (high-priority data traffic from the customer site) with forwarding class af (the af forwarding class is associated with queue 2)

- Precedence is 1
- Forwarding Class is af

vii Click on the OK button. Confirm the action. The association between precedence 1 and the af forwarding class is added to the list.

viii Click on the Create button. The precedence create form opens.

ix Configure the parameters to associate IP precedence 2 (voice traffic from the customer site) with forwarding class l1 (the l1 forwarding class is associated with queue 2):

- Precedence is 2
- Forwarding Class is l1

x Click on the OK button. Confirm the action. The association between precedence 2 and the l1 forwarding class is added to the list.

xi Click on the Create button. The precedence create form opens.

xii Configure the parameters to associate IP precedence 3 (video traffic from the customer site) with forwarding class ef (the ef forwarding class is associated with queue 3)

- Precedence is 3
- Forwarding Class is ef

xiii Click on the OK button. Confirm the action. The association between precedence 3 and the ef forwarding class is added to the list.

23 Click on the Apply button. Confirm the action.

24 Click on the Relations tab to view the associations between the IP precedence bit number, the forwarding class, and the queues.

25 Associate a service SAP with the created High QoS scheduler and the created Premium service access ingress policy. There are many ways to associate policies with L2 or L3 interfaces used as service SAPs, for example, from the service creation form or the port properties form. This sample modifies an existing L2 interface for an existing VPLS.

- **i** Choose Manage→Service→Services from the 5620 SAM main menu. The manage services form opens.
- **ii** Set the filters and click on the Search button. A list of filtered services appears.
- **iii** Select the service and click on the Properties button. The service form opens.
- **iv** Click on the L2 Access Interfaces tab.
- **v** Choose an interface and click on the Properties button. The L2 interface edit form opens.
- **vi** Click on the QoS tab.
- **vii** Configure the parameter. Use the Select button to set the Ingress Policy to Premium service access ingress policy. The policy ID and displayed name appear.
- **viii** Click on the Schedulers tab.
- **ix** Configure the parameter. Use the Select button to set the Ingress Scheduler to High QoS. The displayed name appears.
- **x** Click on the Apply button to save the changes. Confirm the action.

61.6 Workflow to implement QoS on an OmniSwitch

1 Enable QoS on the OmniSwitch and configure global settings such as global port parameters, default disposition for flows, and timeouts. The parameters that you need to configure globally depend on the types of policies that you need to configure.

Typically, you do not need to change any of the global defaults. See step 36 of Procedure 23-63 for information.

2 Configure QoS port parameters, which includes setting QoS parameters on a per port basis. Typically you do not need to change the port defaults. See step 19 of Procedure 16-23 for information.

3 Configure QoS policies. See chapter 43 for more information.

61.7 Workflow to implement QoS on the 7750 SR, 7450 ESS, 7710 SR, 7705 SAR, and 7950 XRS

Planning and configuration

1 Perform network planning activities:

- **i** Determine the required types of services or applications; for example, voice, video, and data.
- **ii** Review SLAs.
- **iii** Perform traffic engineering activities at the IP/MPLS core level to ensure that resources are available.

2 Configure the IP and MAC ACL filters, as required. See Procedures 44-2 and 44-1 for more information.

3 Configure the slope policies. See Procedures 43-8 and 43-10 for more information.

4 Configure the scheduler policies. Scheduler policies can be shared between ingress and egress policies, depending on your specific requirements. See Procedure 43-15 for more information.

5 Configure the port scheduler policies. See Procedure 43-18 for more information.

6 As required, create the aggregation schedulers. See Procedure 43-31 for more information.

7 Configure the access ingress policies. See Procedure 43-1 for more information.

- **i** Configure the forwarding classes.
- **ii** Configure the queues.
- **iii** Map QoS markings on ingress packets to the forwarding classes.
- **iv** Map forwarding classes to the queue definitions.
- **v** Map queue definitions to the scheduler policies.

8 Configure the access egress policies. See Procedure 43-3 for more information.

- **i** Configure the queues.
- **ii** Map forwarding classes to the queue definitions.
- **iii** Map queue definitions to the schedulers policies.

9 Configure the network policies. See Procedure 43-6 for more information.

i Configure for ingress:

- Map QoS markings on ingress packets to the forwarding classes.
- Map forwarding classes to the queue definitions.

ii Configure for egress:

- As required, configure remarking.
- As required, map QoS markings to the forwarding classes.

10 Configure the network queue policies. See Procedure 43-12 for more information.

11 Configure the time of day policies.

i Configure the time ranges. See Procedure 46-1 for more information.

ii Create time of day suites. See Procedure 46-2 for more information.

Application of policies and schedulers to equipment and interfaces

12 Associate the slope policies with ports or daughter cards. See Procedures 16-1 and 15-33 for more information.

13 Associate the network queue policies with MDAs. See Procedures 16-1 and 16-36 for more information.

Configuration of customers and services

14 Configure the customers. See the appropriate service chapter for more information.

15 Create the customer services, and assign policies during the configuration. See the appropriate service chapter for more information.

16 Assign the aggregation schedulers at the interface level, if required. See the appropriate service chapter for more information.

61.8 5620 SAM QoS policies

Policies group and manage the various QoS elements used to determine how traffic is routed.

- access ingress policies
  Specify how QoS marking is interpreted, how customer traffic is mapped into queues, and how queues are classified.
- access egress policies
  Specify how customer traffic is mapped into queues, specify queue classification, queue parameters, and QoS marking.
- network policies
  Specify QoS marking to forwarding class mapping on ingress and QoS marking to forwarding class mapping on egress.

- network queue policies
  Specify CIR, PIR, and burst sizes for each queue. Forwarding class to queue mapping is not configurable.
- scheduler policies
  Specify custom settings and a hierarchical structure of virtual schedulers to replace the default hardware schedulers on the device.
- port scheduler policies
  Specify bandwidth allocation at the egress port level.
- HSMDA scheduler policies
  Specify schedulers to define egress port and ingress scheduler behavior on an HSMDA.
- slope policies
  Specify WRED settings to customize how in-profile and out-of-profile traffic is processed in hardware buffers, applied to daughter cards or ports.
- HSMDA slope policies
  Specify settings for controlling how the depth of HSMDA queues is managed.
- ATM QoS policies
  Specify ATM QoS settings to customize ATM traffic parameters including service category and shaping.

Figure 61-15 shows where QoS policies are applied at the service level.

Figure 61-15 Service-level view of policies

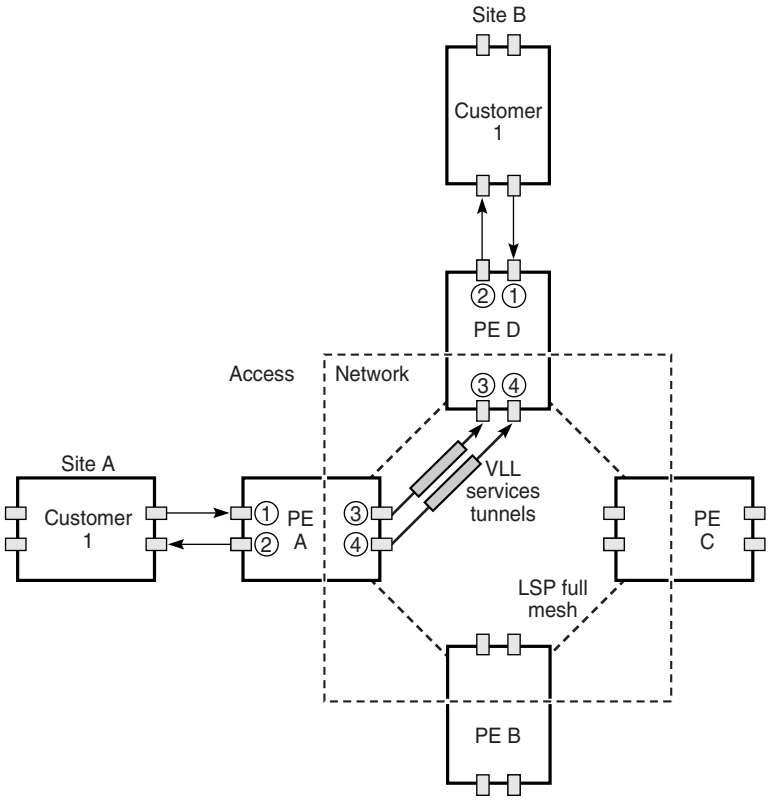
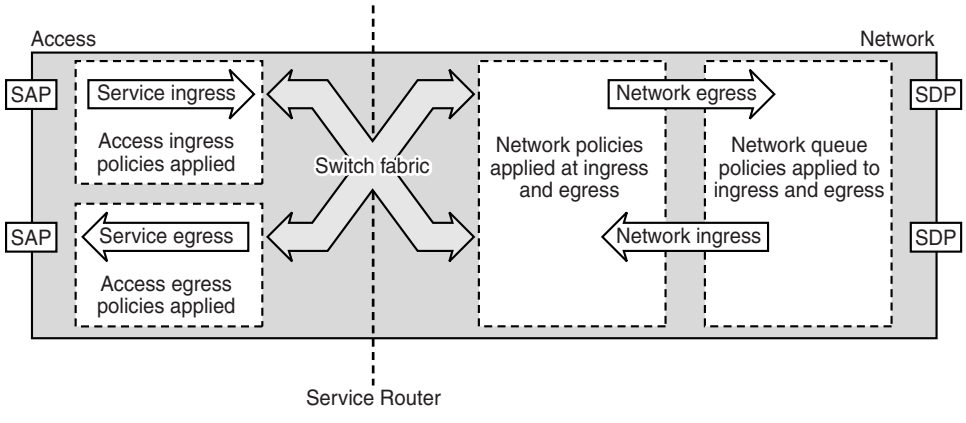


Figure 61-16 shows where policies are applied on a device with respect to access and network ingress and egress traffic.

Figure 61-16 Types of traffic on a device and applied policies



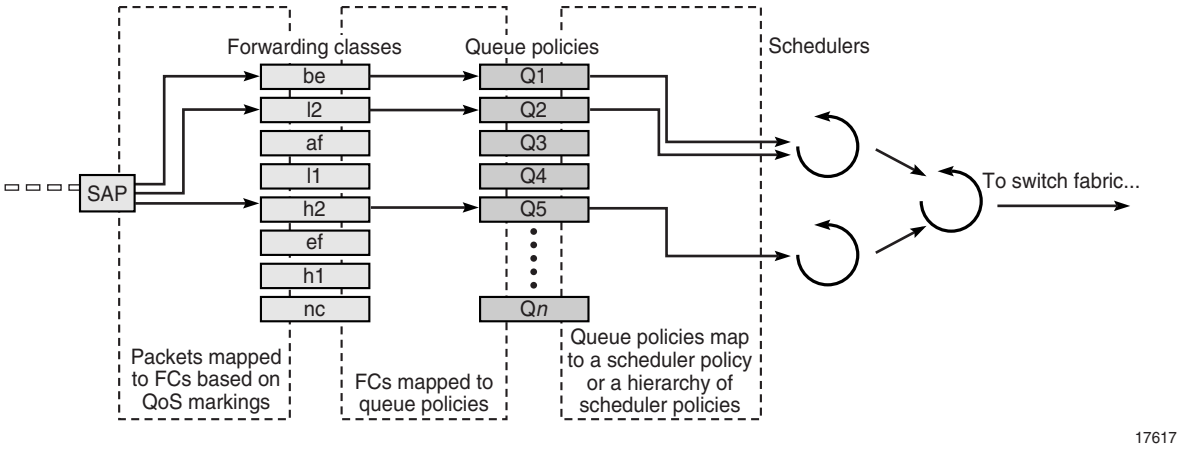
Access ingress policies

Access ingress policies are applied to access interfaces and specify QoS characteristics on ingress. Participation in access ingress policies is defined when access interfaces are configured or modified. Access ingress policies include:

- mapping of QoS marking, such as dot1p, DSCP, and precedence, and IP/MAC address information to forwarding classes
- forwarding class definitions and mapping to queues
- queue definitions and mapping to schedulers

Figure 61-17 shows the access ingress policy elements.

Figure 61-17 Access ingress policy elements



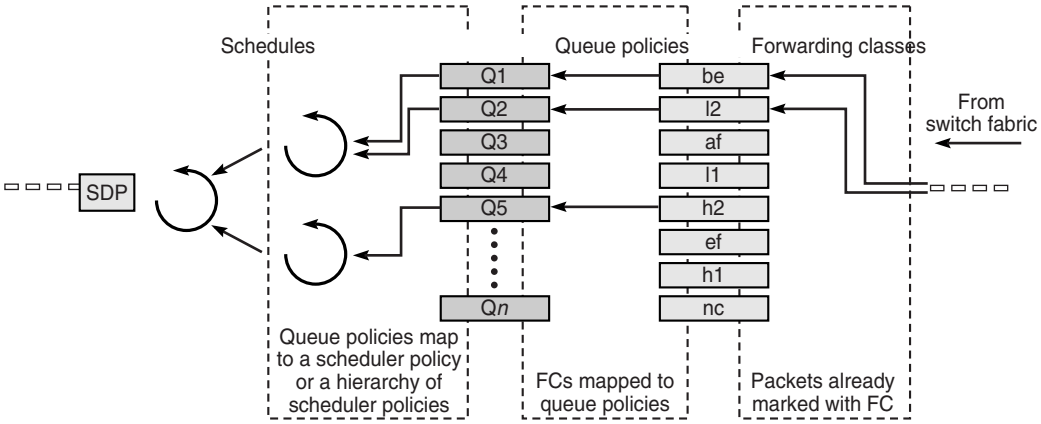
See "Access ingress policies" in section 43.1 for more information about access ingress policies.

Access egress policies

Access egress policies are applied to access egress interfaces and specify QoS characteristics on egress. Participation in Access egress policies is defined when access interfaces are configured or modified. Access egress policies include:

- forwarding class definitions and mapping to queues
- queue definitions and mapping to schedulers

Figure 61-18 Access egress policy elements



In Figure 61-18, packets are marked with an FC, either by:

- ingress policy if the packet was received on the same device
- in the tunnel transport encapsulation if received using a service tunnel

See "Access egress policies" in section 43.1 for more information.

Network policies

Network policies define egress QoS markings and ingress QoS interpretation for traffic on core network IP interfaces. A network policy defines:

- DSCP name mapping to forwarding classes
- LSP EXP value mappings to forwarding classes
- whether QoS remarking is enabled

Figure 61-19 shows the sequence of how the elements of network and network queue policies are applied at ingress.

Figure 61-19 Network and network queue policy elements on ingress

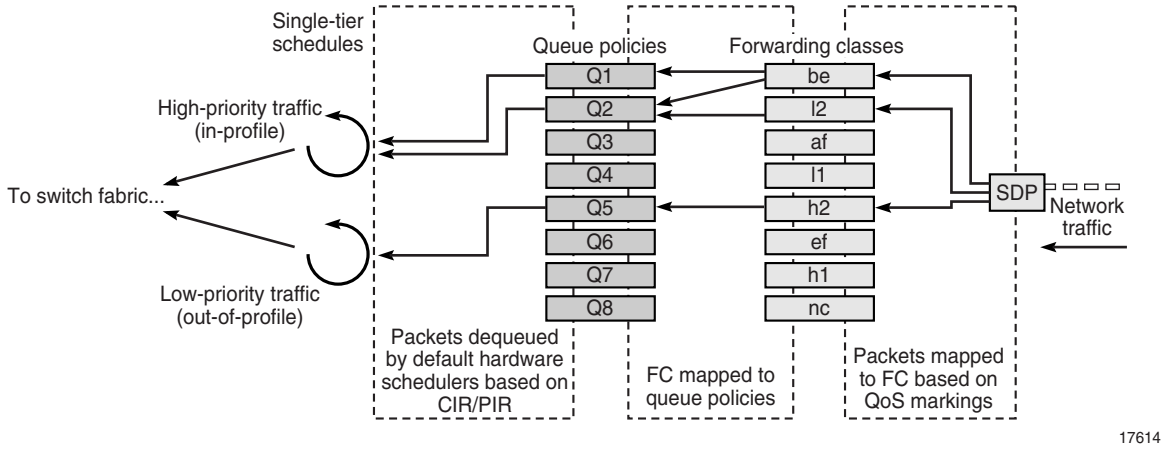
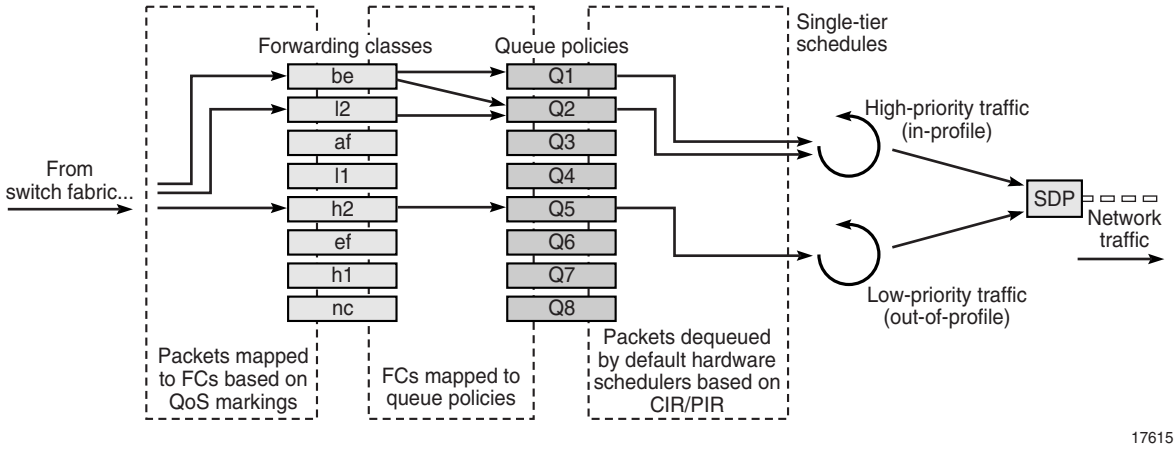


Figure 61-20 shows the sequence of how the elements of network and network queue policies are applied at egress.

Figure 61-20 Network and network queue policy elements on egress



See "Network policies" in section 43.1 for more information.

Network queue policies

Network queue policies define the network forwarding class queue characteristics for core egress network ports and for ingress on MDAs.

See Figure 61-19 and Figure 61-20 for the sequence of how the different elements of network and network queue policies are applied on ingress in and on egress.

The queued packets are serviced by single-tier schedulers on the device and are forwarded to a single destination switch fabric port or a network interface.

See "Network queue policies" in section 43.1 for more information about network queue policies.

Scheduling

Scheduling defines the order and method for how packets which are enqueued in different queues, are dequeued. Ingress schedulers control the data transfer between the queues and the switch fabric. Egress schedulers control the data transfer between the egress queues and the switch fabric. Packets are not actually forwarded to schedulers, but are forwarded from the queues directly to ingress and egress interfaces. Participation in scheduler policies is defined when access interfaces are configured or modified. There are two types of scheduling:

- Single-tier scheduling is the hardware-based default method for scheduling queues on the device. There are no configurable parameters for single-tier schedulers. When a scheduler policy is not specified for an access interface, rate limiting is specified by the values specified in the queue and scheduling is performed by the default hardware scheduler on the device. Single-tier scheduling consists of a pair of scheduling priority loops in the 7750 SR and bases scheduling on the CIR and the PIR set in the queue policy. One loop is for scheduling high-priority (in-profile) traffic, and the other loop is for low-priority (out-of-profile) traffic.
- Virtual hierarchical (multi-tier) scheduling can provide more flexible scheduling for access ingress and egress interfaces, and determine how queues are scheduled. They are defined using a Scheduler policy, and can be configured to override default hardware scheduling. You can create up to three tiers of virtual schedulers.

  Aggregation schedulers are used to share a scheduler policy across a number of ports or daughter cards. This can be useful when a number of ports or cards are dedicated to the same customer. See "Scheduler policies" in section 43.1 for more information about configuring aggregation schedulers.

Port scheduler policies

Port scheduler policies define the bandwidth allocation based on the available bandwidth at the egress port level. A port scheduler policy manages a bandwidth allocation algorithm that represents a virtual multi-tier scheduling hierarchy.

The port scheduler allocates bandwidth to each service or subscriber that is associated with an egress port. Egress queues on the service may have a child association with a scheduler policy on the SAP or multi-service site. All queues must compete for bandwidth from an egress port. There are two methods of bandwidth allocation on the egress access port:

- **direct association of port scheduler on a SAP or multi-service site with service or subscriber queue**

  A service or subscriber queue is associated with a scheduler on the L2 access interface or multi-service site, and the service-level scheduler policy is associated with a port level scheduler.
- **direct association of port scheduler with service or subscriber queue**

  A service or subscriber queue is associated with a port scheduler. The port scheduler hierarchy allocates bandwidth at each priority level to each service or subscriber queue.

See "Port scheduler policies" in section 43.1 for more information about configuring port scheduler policies.

HSMDA scheduler policies

The port-based scheduler manages forwarding for each egress port on the HSDMA. Each port-based scheduler maintains up to eight forwarding levels. Eight scheduling classes contain each of the queues that are assigned to the port scheduler. Membership in a scheduler is defined by the queue identifier.

The port-based scheduler supports a port-based shaper that is used to create a sub-rate condition on the port. Each scheduling level can be configured with a shaping rate to limit the amount of bandwidth allowed for that level.

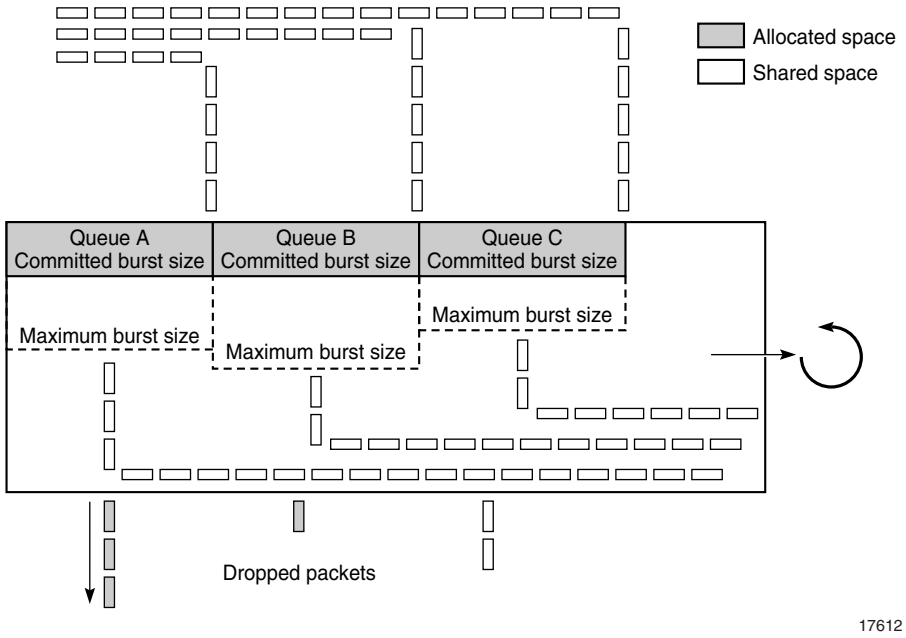
The port-based scheduler allows two weighted groups (group 1 and group 2) to be created. Each group can be populated with three consecutive scheduling classes.

See "HSMDA scheduler policies" in section 43.1 for more information about configuring slope policies.

Slope policies

Slope policies manage how shared buffers are utilized on the SR. When traffic is queued, the WRED slope parameters in the slope policy determine how the traffic is buffered for dequeuing, as shown in Figure 61-21.

Figure 61-21 Slope policy characteristics



All queues are in contention for shared buffer space when they exceed their CBS, and can use their MBS, when space is available in the shared buffer space. The WRED parameters determine whether a packet is discarded or not, and, as a result, determine whether the packet is dequeued. When the shared buffer space exceeds or approaches the maximum percentage defined by the WRED configuration, packets are discarded.

By using two independent slope policy configurations, one for in-profile traffic and one for out-of-profile traffic, you can configure in-profile traffic to receive preferential treatment over out-of-profile traffic.

See "Slope policies" in section 43.1 for more information about configuring slope policies.

HSMDA slope policies

HSMDA slope policies control the HSMDA queues. Each queue supports an index for an HSMDA slope policy table. Each policy in the table consists of two RED slopes (one high priority and another for low priority) to manage queue congestion. HSMDA RED slopes operate on the instantaneous depth of the queue.

A packet that attempts to enter a queue triggers a check to see whether the packet is allowed based on queue congestion conditions. The packet contains a congestion-priority flag that indicates whether the HSMDA is to use the high or low slope. The slope policy containing the slope is derived from the policy index in the queue configuration parameters on the HSMDA.

The RED slope discards are based on the current queue depth before a packet is allowed into the queue. Therefore, a queue may consume buffers that are greater than the configured MBS value based on the size of the packet. After the packet maximum is reached, packets that are associated with the queue are discarded. When the schedule removes packets from the queue, the queue depth decreases, which eventually lowers the depth of the threshold.

See "HSMDA slope policies" in section 43.1 for more information about configuring HSMDA slope policies.

62 — Queue groups

62.1 Queue group overview *62-2*

62.2 Workflow to configure access SAP forwarding class-based redirection *62-6*

62.3 Workflow to configure network IP interface forwarding class-based redirection *62-7*

62.4 Workflow to configure statistics collection for queue groups *62-8*

62.1 Queue group overview

Queue groups are objects created on access or network Ethernet ports that allow SAP or IP interface forwarding classes to be redirected from standard queue mapping to a shared queue. Access ingress ports support a single queue group for each ingress port. Access egress and network egress ports support the creation of multiple queue groups. Shared queuing is supported on the 7450 ESS, 7710 SR, Release 7.0 R3 or later, and the 7750 SR.

Queue Group Template policies

Queue Group Template policies allow you to define the queuing and parenting structure for queue groups on Ethernet ports. The policy defines the number and types of queues within the port queue group, and provides the default queue parameters.

Before you create a queue group on an Ethernet port, you must first create a Queue Group Template.

See "Queue Group Template policies" in section 43.1 for more information.

Port queue groups

The port queue group contains the queue groups that are created based on the queue IDs defined within the associated Ingress/Egress Queue Group Template policies. Port queue groups are supported on Ethernet ports and can be created on ports within a LAG. Port queue groups are not supported on HSMDA Ethernet ports and VSM MDAs. Network egress queue groups are not supported on the following IOM-1 cards:

- IOM-10 G
- IOM-20 G
- IOM-20 G-B

You can create a port queue group on an Ethernet port after creating an Ingress/Egress Queue Group Template policy.



Note — You must use the same name for the port queue group and Ingress/Egress Queue Group Template policy.

Port queue group LAGs

When a port queue group is created on a LAG, the group is individually instantiated on each link in the LAG. The queue parameters for a queue within the queue group are used for each port queue.

You can create, modify, or delete a port access ingress, access egress, or network egress queue group on the primary port of the LAG. (The primary port is the port with the lowest port ID.) The NE automatically replicates the create, modify, or delete action for the queue group on all other ports within the LAG.



Note — The 5620 SAM does not allow you to create, modify, or delete an Access Ingress, Access Egress, or Network Egress queue groups on non-primary ports.

When you add a port to a LAG, the port must use the same access ingress, access egress, or network egress queue groups as the existing ports on the LAG. To ensure this requirement for the port, the 5620 SAM implements the following sequential comparison:

- number of queue groups
- queue group names
- queue group Instance IDs
- number of queue overrides
- individual parameters



Note — Alcatel-Lucent recommends that you add all required ports to the LAGs before the configuration of the port queue group.

In the services context, the following requirements must be observed:

- For any service SAP that associates its connection to a LAG, the forwarding plane must exist on the card for the LAG's primary port to be selectable.
- Whenever you add a port from a different card to a LAG, the forwarding plane redirect name and associated Instance ID parameters you configure must be identical to those that have already been configured for the service.

Access SAP forwarding class-based redirection

Typically, each SAP has dedicated ingress and egress queues that are only used by that specific SAP. Individual SAP queuing requires a more complex provisioning model to configure the ingress and egress SLAs of the SAP. The configuration requires service awareness at the aggregation locations in the network. There are cases where individual SAP queuing is not preferred. In these cases, you can use a shared queue or an individual port queue model. You can configure a shared queue by creating access ingress and access egress queue groups, and mapping the forwarding classes of the SAP to the queues within the queue group.

You can configure forwarding class redirection on a SAP to a queue group queue ID using the access ingress/egress QoS policy. In each policy, the forwarding class to queue ID mapping can specify a queue group name.

See section 62.2 for more information.

Network IP interface forwarding class-based redirection

You can create queue groups on egress network ports to provide network IP interface queue redirection. A single set of egress port-based forwarding class queues are available by default, and all IP interfaces on the port share the queues. The creation of a network queue group allows one or more IP interfaces to selectively redirect forwarding classes to the group to override the default behavior.

The redirection of the egress forwarding class on an IP interface to an egress queue group queue ID is provisioned using the Network policy. The actual queue group name can be specified when the Network Policy is applied to the IP interfaces.

You can configure dedicated queues for each IP interface using network egress queue groups.

See section 62.3 for more information.

Queue group statistics

The packets sent to the queue of a SAP are statistically tracked by a set of counters associated with the queue group queue, not the SAP counters. The tracking occurs when a forwarding class is redirected to an ingress or egress port queue group queue.

On a network interface, the counter sets are created for each egress IP interface, not for each egress queue. The same counter set is used when a forwarding class for an egress IP interface is redirected from the default egress port queue to a queue group queue.

See “Statistics collection overview” in the *5620 SAM Statistics Management Guide* for information about managing statistics collection and to view a list of the MIB counters that are available for collection using the 5620 SAM.

Queue group configuration validation rules

Table 62-1 describes the validation rules that are enforced for NE queue group configurations.

Table 62-1 Validation requirements for queue group configurations

Component		Validation action
Ingress Queue Group Template policy	Queue deletion	The deletion is blocked if there is an Access Ingress QoS policy with a forwarding class that is associated with the queue ID. The deletion can be blocked by the 5620 SAM or the NE. You can use the name binding list to verify dependencies.
	Policy deletion	The deletion is blocked if there is an Access Ingress QoS policy with a forwarding class that is associated with the policy.

(1 of 3)

Component		Validation action
Egress Queue Group Template policy	Queue deletion	The deletion is blocked if there is an Access Egress QoS policy with a forwarding class that is associated with the queue ID. The deletion can be blocked by the 5620 SAM or the NE. You can use the name binding list to verify dependencies.
		The deletion is blocked if there is a Network policy with a forwarding class that is associated with the queue ID.
	Policy deletion	The deletion is blocked if there is an Access Egress QoS policy with a forwarding class that is associated with the policy.
		The deletion is blocked if there is a network IP interface associated with the policy.
Port queue groups	Port Access Ingress Queue Group deletion	The deletion is blocked if there is an Access Ingress QoS policy, applied to the SAP, with a forwarding class that is associated with the port queue group. The SAP is directly or indirectly bound to the port by a LAG associated with the port queue group.
	Port Access Egress Queue Group	The deletion is blocked if there is an Access Egress QoS policy, applied to the SAP, with a forwarding class that is associated with the port queue group. The SAP is directly or indirectly bound to the port by a LAG associated with the port queue group.
	Network Egress Queue Group	The deletion is blocked if there is a network IP interface that is directly or indirectly bound to the port by a LAG associated with the port queue group.
Access SAP forwarding class-based redirection	Access Ingress QoS policy	The Queue Group name must exist as an Ingress Queue Group Templates policy.
		The Queue ID must exist within the associated Ingress Queue Group Templates policy with appropriate queue type.
		Only one unique Queue Group may be referenced within one Access Ingress QoS policy.
		The current Access Ingress QoS policy should not be applied to the SAPs on a non-Ethernet port or an Ethernet port where the specified Access Ingress Queue Group does not exist.
		The current Access Ingress QoS policy should not be applied to a SLA Profile policy.
	Access Egress QoS policy	The Queue Group name must exist as an Egress Queue Group Templates policy.
		The Queue ID must exist within the associated Egress Queue Group Templates policy.
		The current Access Egress QoS policy should not be applied to the SAPs on a non-Ethernet port or an Ethernet port where the specified Access Egress Queue Group does not exist.
		The current Access Egress QoS policy should not be applied to a SLA Profile policy.
	Access Ingress/Egress QoS policy assignment	When an Access Ingress/Egress QoS policy with a forwarding class redirection to a Queue Group Queue ID is applied to a SAP, the following configurations are verified: • The Queue Group specified in any forwarding class redirection must exist as an Access Ingress/Egress Queue Group on the port associated with the SAP • The Access Ingress/Egress QoS policy with Queue Group specified cannot be applied to SLA Profile policy

(2 of 3)

Component		Validation action
Network IP Interface forwarding class-based redirection	Network policy	The specified queue ID must exist within the Egress Queue Group Templates policy for all IP interfaces where the Network policy is applied. If the Network policy is currently applied to any IP interfaces without an explicit Network Egress Queue Group specified, the configuration fails.
		The following configurations are verified when the Network policy is applied to a network IP interface: • The network policy with a redirected queue group cannot be applied to the network IP interface without a port binding. • The redirected queue group name must exist as a Network Egress Queue Group on the port or LAG associated with the IP interface. • The queue ID for the redirected queue group in the associated Network policy must exist within the associated Egress Queue Group Templates policy.

(3 of 3)

62.2 Workflow to configure access SAP forwarding class-based redirection

The following workflow describes the steps required to configure access SAP forwarding class-based redirection.

1 Create a global ingress/egress queue group template policy, as required.

   a Create an ingress queue group template policy. See Procedure 43-23 for more information.

   b Create an egress queue group template policy. See Procedure 43-24 for more information.

2 Distribute the global ingress/egress queue group template policy to the NEs. See Procedure 42-1 for more information.

3 Create an ingress/egress queue group on the Ethernet access port. See Procedure 16-8 for more information.

4 Create or configure a global access ingress/egress QoS policy with the forwarding class mapped to the queue group queue ID. The queue group queue ID must be included in the queue group template policy. Perform the following, as required:

   a Create an access ingress QoS policy. See Procedure 43-1 for more information.

   b Create an access egress QoS policy. See Procedure 43-3 for more information.

5 Distribute the global access ingress/egress QoS policy to the NEs. See Procedure 42-1 for more information.

6 On the SAP configuration form, assign the access ingress/egress QoS policy to the SAP bound to the port on which the access ingress/egress queue group was created in step 3. Perform one of the following, as required:

   a Assign an access ingress/egress QoS policy to an L2 access interface on a VLL. See Procedure 67-28 for more information.

   b Assign an access ingress/egress QoS policy to an L2 access interface on a VPLS. See Procedures 68-24, 68-66, and 68-70 for more information.

   c Assign an access ingress/egress QoS policy to an L3 access interface on an IES. See Procedure 70-17 for more information.

   d Assign an access ingress/egress QoS policy to an L3 access interface on a VPRN. See Procedure 71-22 for more information.

62.3 Workflow to configure network IP interface forwarding class-based redirection

The following workflow describes the steps required to configure a network IP interface forwarding class-based redirection.

1 Create a new global egress queue group template policy. See Procedure 43-24 for more information.

2 Distribute the global egress queue group template policy to the NEs. See Procedure 42-1 for more information.

3 Create an egress queue group on the Ethernet network port. See Procedure 16-8 for more information.

4 Create or configure a global network policy with the forwarding class mapped to the queue group queue ID. The queue group queue ID must be included in the egress queue group template policy, which is specified when the network policy is applied to the IP interface. See Procedure 43-6 for more information.

5 Distribute the global network policy to the NEs. See Procedure 42-1 for more information.

6 On the network interface configuration form, assign the network policy and the queue group template policy to the network interface. The network egress queue group must be created on the port to which the network interface is bound. The network egress queue group must use the same name as the selected queue group template policy. See Procedure 22-9 for more information.

62.4 Workflow to configure statistics collection for queue groups

The following workflow describes the steps required to enable the collection of queue groups statistics.

1 Create or modify an accounting policy. See “To create or modify an accounting policy” in the *5620 SAM Statistics Management Guide* for more information.

2 Configure the Type parameter on the Accounting Policy form to collect one of the following statistics options:

- Combined Queue Group
- Queue Group Octets
- Queue Group Packets

3 Enable the Collect Accounting Statistics parameter on the port’s queue group Physical Port (Edit) form. See Procedure 16-8 for more information about adding an access ingress/egress queue group on an Ethernet access port.

63 — Virtual ports

63.1 Virtual port overview *63-2*

63.2 Workflow to configure and manage virtual ports *63-3*

63.3 Virtual ports procedures *63-3*

63.1 Virtual port overview

A 7750 SR can act as a Broadband Network Gateway (BNG), fairly distributing bandwidth among the subscriber host sessions by accounting for the packet encapsulation overhead and ATM bandwidth expansion for each type of broadband session. In this way, subscriber packets are less likely to be dropped downstream in the DSLAM DSL port. Furthermore, the BNG shapes the aggregate rate of each subscriber and the aggregate rate of all subscribers destined to a given DSLAM to prevent congestion of the DSLAM.

In the BNG application, when a set of per FC queues are applied to each subscriber host context, the host per FC queue packet rate is overridden by the rate provided in the Radius access-accept message. This rate represents the ATM rate that will be seen on the last mile and includes the encapsulation offset and the per packet expansion due to ATM segmentation into cells at the BSAN.

In order to enforce the aggregate rate of each destination BSAN, a virtual port must be configured. Virtual ports are scheduling nodes that operate like port schedulers, with the exception that multiple virtual ports can be created on the egress context of an access/hybrid Ethernet port. A virtual port and a port scheduler cannot exist simultaneously on a single port.

Virtual ports can be configured on a port that is a member of a LAG. When a virtual port is created, modified, or deleted on the primary port of a LAG, this action is replicated on all other ports within the LAG. These actions can only be performed on the primary port. When a port is added to a LAG, it must have the same virtual ports defined as the existing ports on the LAG. The name of a virtual port is local to the port on which it is applied, but must be the same for all member ports of a LAG.

Virtual ports are supported on Ethernet ports on IOM3/IMM on the 7750 SR, 7750 SR-c4, and 7450 ESS.

Virtual ports are not supported on the 7750 SR-1 and the 7450 ESS-1, HSMDA Ethernet ports, or VSM MDA.

Virtual port statistics can be collected and displayed for all queues forwarding to a virtual port configured on an egress of an Ethernet port. This is only supported on an 7750 SR or 7450 ESS equipped with a 2 x XP MDA IOM-3. The collected data is available on the Statistics tab of the Egress Scheduling Virtual Port properties form.

SLA Profiles

A subscriber host queue with the port-parent option enabled can be scheduled within the context of a port scheduler policy associated with a port or a virtual port. To specify that a subscriber host queue with the port-parent option enabled be scheduled within the context of a virtual port, the Scheduler Type parameter must be set to Virtual port when configuring an SLA Profile.

See Procedure 54-17 for more information.

Subscriber Profiles

The subscriber aggregate rate is adjusted to account for the fixed offset and per packet variable expansion of the last mile for the specific session used by the subscriber host. The adjustment is based on the average frame size.

See Procedure 54-18 for more information.

63.2 Workflow to configure and manage virtual ports

The following workflow describes the steps required to configure and manage virtual ports.

1 Configure an SLA Profile, as described in Procedure 54-17.

2 Configure a Subscriber Profile, as described in Procedure 54-18.

3 Configure virtual ports, as required.

   a Configure a virtual port using the navigation tree, as described in Procedure 63-1.

   b Configure a virtual port using the Port QoS form, as described in Procedure 63-2.

   c Copy a virtual port using the Port QoS form, as described in Procedure 63-3.

63.3 Virtual ports procedures

The following procedures describe how to configure and manage virtual ports.

Procedure 63-1 To configure a virtual port using the navigation tree

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device type (applies to ports on the IOM3 and IMM on the 7750 SR, 7750 SR-c4 and 7450 ESS) where you want to configure virtual ports and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Expand the Shelf icon in the navigation tree. Expand to the port level and click on an access/hybrid Ethernet port. The Port form opens with the General tab displayed

4 Click on the Egress Scheduling Virtual Port tab.

5 Click on the Create button. The Egress Scheduling Virtual Port (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Name
- Description

7 Click on the Select button in the Port Scheduler Policy panel and choose a port scheduler policy from the Select Port Scheduler Policy form.



Note — You cannot select a port scheduler policy for the virtual port if you have already selected a port scheduler policy for the associated channel. Likewise, selecting a port scheduler policy for the virtual port prevents you from selecting a port scheduler policy for the associated channel.

8 Select the Assign Aggregate Rate Limit check box on the Aggregate Rate Limit panel before you define the Aggregate Rate Limit (kbps).

9 Configure the Status parameter in the Egress Rate Modify panel.

10 Click on the Host Matching tab.

11 Click on the Create button. The Host Matching form opens.

12 Configure the Destination String parameter.

13 Click on the OK button. A confirmation dialog box appears.

14 Click on the OK button. The Egress Scheduling Virtual Port (Create) form reappears with the Destination String information displayed.

15 Click on the OK button. A dialog box appears.

16 Click on the OK button. The Port form reappears with the Egress Scheduling Virtual Port information displayed.

17 Click on the OK button. A confirmation dialog box appears.

18 Click on the Yes button. The Port form closes.

Procedure 63-2 To configure a virtual port using the Port QoS form

1 Choose Manage→Equipment→Port QoS from the 5620 SAM main menu. The Manage Port QoS list form opens.

2 Select Egress Scheduling Virtual Port (Physical Equipment) from the object type drop-down list.

3 Click on the Add button and choose Virtual Port(s). The Egress Scheduling Virtual Port (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Name
- Description

5 Click on the Select button in the Port Scheduler Policy panel and choose a port scheduler policy from the Select Port Scheduler Policy form.

6 Select the Assign Aggregate Rate Limit check box on the Aggregate Rate Limit panel before you define the Aggregate Rate Limit (kbps).

7 Configure the Status parameter in the Egress Rate Modify panel.

8 Click on the Host Matching tab.

9 Click on the Create button. The Host Matching form opens.

10 Configure the Destination String parameter.

11 Click on the OK button. A confirmation dialog box appears. Click on OK.

12 Click on the Targeted Physical Ports tab.

13 Click on the Add button. The Select Site form opens.

14 Click on the Search button. The form displays a list of sites.



Note — The count displayed on the form reflects the total number of found ports and may not align with the number of applicable ports displayed in the list.

15 Select a site in the list and click on the OK button. The Select Site form closes and the Egress Scheduling Virtual Port (Create) form reappears with the site information displayed.

16 Click on the OK button. The Egress Scheduling Virtual Port (Create) form closes and the Port QoS list form reappears.

17 Close the form.

Procedure 63-3 To copy a virtual port

1 Choose Manage→Equipment→Port QoS from the 5620 SAM main menu. The Port QoS list form opens.

2 Select Egress Scheduling Virtual Port from the object type drop-down list.

3 Click on the Search button. The form displays a list of virtual ports.

4 Select a virtual port in the list and click on the Copy button. The Egress Scheduling Virtual Port (Create) form opens with the virtual port's values populated.

5 Click on the Targeted Physical Ports tab.

6 Click on the Add button. The Select Site form opens.

7 Click on the Search button. The form displays a list of sites.

8 Select one or more sites in the list and click on the OK button. The Select Site form closes and the Egress Scheduling Virtual Port (Create) form reappears with the site information displayed.

9 Click on the OK button. The Egress Scheduling Virtual Port (Create) form closes and the Port QoS list form reappears.

10 Close the form.

64 — Customer configuration and service management

64.1 Customer configuration and service management overview *64-2*

64.2 Workflow to create a customer profile and manage customer services *64-3*

64.3 Customer configuration and service management procedures *64-3*

64.1 Customer configuration and service management overview

The 5620 SAM allows you to create a customer profile and manage the services the customer subscribes to.

An end user is the recipient of application content that is delivered through a service. The service is a means of transport for the application content and is owned by a service customer. For example, an end user subscribes to a high-speed Internet access service, and the Internet access service is owned by a service provider who is a service customer of the network provider. The 5620 SAM provides only customer management, not end-user management. Customers were called subscribers in earlier releases of 5620 SAM.

On the General tab of a customer management form, you can configure basic customer information. From the other tabs on the form, you can configure and monitor 5670 RAM thresholds, services, service sites, templates, and aggregation schedulers for a customer.

Each customer is associated with an ID that is assigned when the customer account is created. When configuring a service, you can use the ID or the listed name of the customer to associate a customer with a service.

A customer can own more than one service, but an individual service is owned by only one customer. Two or more services can be joined to form a composite service. The individual services that comprise the composite service can be owned by different customers. Customers that own services participating in a composite service are associated with the composite service.

Managing the size of a service associated with a customer

A customer service can become very large over time if new sites are continually added. As a result, a service containing thousands of sites or instances may become cumbersome to manage. The 5620 SAM allows you to easily move sites from one service to another in order to reduce the overall size of a particular service.

Sites can be moved for the following service types supported in 5620 SAM: VPRN, VPLS, MVPLS, IES, and all VLL types. However, the following restrictions apply:

- You can only move a site between like services, that is, from one VPLS to another VPLS, but not between a VPLS and a VPRN, for instance.
- The services that you are moving sites to and from must have the same Service ID.
- The services that you are moving sites to and from must have the same Customer ID.

If you need to reduce the size of an existing service, you can use another existing service that meets these restrictions. Alternatively, you can create a new service of the same type for this purpose. The Service ID and Customer ID of the new service must match those of the existing service.

In addition, if the existing service which you are moving sites from is a member of a composite service, then the newly-created service you are moving the sites to will also belong to the same composite service. This action will only take place after moving the sites that form the composite service connectors. See Procedure 64-5 for more information about how to move sites from one service to another.

64.2 Workflow to create a customer profile and manage customer services

1. Create a customer profile. See Procedure 64-1.
   a. Configure or modify key customer contact and billing information.
   b. Assign or associate equipment or resources to the customer, as appropriate.
2. As required, configure the system preferences of services associated with a customer such as specifying the default service priority or the automatic removal of empty service. See "To configure 5620 SAM system preferences" in the *5620 SAM System Administrator Guide* for more information.
3. Create, modify, or delete existing services such as IES, VPLS, VPRN, or VLL that are associated with customers. See the relevant service chapter in this guide.
4. Monitor or troubleshoot customers, based on SLAs between the customer and the service provider.
   a. Retrieve customer information and contact the customer when service problems or maintenance windows occur. See Procedure 64-2.
   b. View a service map for a customer. See Procedure 64-3.
   c. Perform diagnostics as appropriate to troubleshoot service problems associated with customers. See the relevant service chapter in this guide.
   d. As required, view and modify the inventory of all the services, interfaces, circuits, and other information that are associated with a customer. See Procedure 64-4.
   e. If required, reduce the service size associated with a customer by moving sites from one service to another. See Procedure 64-5.
5. As required, delete a customer from the 5620 SAM database. See Procedure 64-6.

64.3 Customer configuration and service management procedures

The following procedures describe how to configure and manage customers and the various aspects of their services. Detailed procedures on specific service type creation and modification are provided in the relevant service chapters.

Procedure 64-1 To create a customer profile

1. Choose Manage→Service→Customers from the 5620 SAM main menu.
2. Click on the Create button. The Customer (Create) form opens with the General tab displayed. The General tab shows contact and billing information.

3 Configure the parameters.

- Auto-Assign ID
- ID
- Name
- Description
- Address
- Phone Number
- Contact
- Email

The information in the General tab is used to create a database of customer information, including contact information, so that the customer can be contacted if there is a service or equipment problem.

4 As appropriate, configure any other tabs on the Customer (Create) form. See step 5 in Procedure 64-4.

5 Click on the Apply button to save the customer information.

Procedure 64-2 To list the services associated with a customer

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens with Service (Service Management) selected in the filter list.

2 Use the filter for the Customer Name column to filter the list results.

3 Click on the Search button. A list of services matching the filter criterion appears.

Procedure 64-3 To view a service map for a customer

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Choose Service (Service Management) from the object drop-down list.

3 Use the filter for the Customer Name column to filter the list results.

4 Click on the Search button. A list of services matching the filter criterion appears.

5 Choose a service from the list and click on the Topology View button. A dialog box appears.

6 Click on the Yes button. The Service Topology - *Service Name* form opens.

7 Scroll the map to view the topology of the service and the devices used for the service.

8 Click on the Close button to close the map.

Procedure 64-4 To modify and manage customer information

Use this procedure to view and modify the inventory of all the services, interfaces, circuits, and other information that are associated with a customer.

1 Choose Manage→Service→Customers from the 5620 SAM main menu. The Manage Customers form opens.

2 Click on the Search button to search for the customer whose information you want to change. The search results are displayed in the bottom panel of the form.

3 Choose the customer and click on the Properties button. The Customer (Edit) form opens.

4 View or modify the information for the customer.

Each tab lists parameters you can view or modify, or functions that you can perform, related to customer management.

- The General tab lists the ID, the customer name, and contact information.
- The 5670 RAM Parameters lists the Apdex and MOS thresholds that can be set by the customer. See step 5b for more information.
- The Services tab lists which services such as VPLS, VPRN, or VLL are associated with the customer.
- The Sites tab lists the PE devices used by the customer.
- The Aggregation tab lists aggregation schedulers defined for the customer. See chapter 43 for information about creating aggregation schedulers.
- The Associated Templates tab lists service templates used to create services for the customer.
- The Spans tab lists the span of control over customers.

5 Modify customer information as appropriate:

a To modify text in the General tab:

i Make the changes in the appropriate fields and click on the OK button. A dialog box appears.

ii Click on the Yes button. The Customer (Edit) form closes.

b Configure the 5670 RAM parameters as listed below:

- Reporting Name
- Apdex Thresholds - Unacceptable
- Apdex Thresholds - Poor
- Apdex Thresholds - Fair
- Apdex Thresholds - Good
- MOS Thresholds - Unacceptable
- MOS Thresholds - Poor
- MOS Thresholds - Fair
- MOS Thresholds - Good

c To modify site or template information for the customer:

i Click on the appropriate tab on the Customer (Edit) form.

ii Select the object in the list for which you want to modify information.

iii Click on the Properties button. The configuration form for the object opens.



Caution — Ensure configuration changes do not affect customer services. Use the Turn Down button to turn down a service before making any changes that may affect customer traffic.

iv Modify the information on the configuration form as required and click on the OK button. The changes are saved and the object configuration form closes.

Procedure 64-5 To move sites from one service to another

Sites can be moved for the following service types supported in 5620 SAM: VPRN, VPLS, MVPLS, IES, and all VLL types. However, the following restrictions apply:

- You can only move a site between like services, that is, from one VPLS to another VPLS, but not between a VPLS and a VPRN, for example.
- The services that you are moving sites to and from must have the same Service ID.
- The services that you are moving sites to and from must have the same Customer ID.

See "Managing the size of a service associated with a customer" in this chapter, for more information.



Note 1 — When you perform a service size reduction, the 5620 SAM does not create a composite service for services that have only mesh SDP bindings.

Note 2 — See chapter 74 for more information about composite services.

1 To move more than 25 sites at a time, go to step 2. Otherwise, go to step 5.

2 Choose Administration→System Preferences from the 5620 SAM main menu. The System Preferences form opens.

3 Configure the Auto Discover Composite Services parameter. The maximum number of sites you can move at a time is 50.



Note — The Auto Discover Composite Services parameter can be modified only by a user with administration privileges.

4 Click on the OK button. The System Preferences form closes.

5 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

6 Choose Service (Service Management) from the object drop-down list.

7 Click on the Search button. A list of available services is displayed.

8 Choose the service from which you want to move the sites and click on the Properties button. The *Service* (Edit) form opens with the General tab displayed.

9 In the service navigation tree, expand the Sites icon to view the sites in the service.

10 Right-click on the site you want to move and choose Move to Another Service from the contextual menu. A dialog box appears.

11 Click on the Yes button. The Select Services form opens and displays a list of applicable services to which you can move the selected site.

12 Choose the required service and click on the OK button. A progress message is displayed, followed by a confirmation message, after the move is complete and the 5620 SAM creates a composite service.

13 To view the composite service that is automatically created by the 5620 SAM after a successful move, click on the Properties button in the Composite Service panel. The Composite Service (Edit) form opens with the General tab displayed.

14 Close the Composite Service (Edit) form.

15 Close the *Service* (Edit) form.

Procedure 64-6 To delete customers



Note — You cannot delete customers that have associated services.

1 Choose Manage→Service→Customers from the 5620 SAM main menu. The Manage Customers form opens.

2 Search for the customer that you want to delete. The search results are displayed in the bottom panel of the form.

3 Choose the customer from the list and click on the Delete button. A Confirm dialog box appears.



Caution — Removing a customer deletes all information associated with the customer. Ensure that the correct customer has been selected.

4 Perform one of the following:

a Click on the No button to avoid deleting the customer. The Confirm dialog box closes.

b Click on the Yes button. The customer is deleted from the 5620 SAM database.

65 — Residential subscriber management

65.1 Residential subscriber overview *65-2*

65.2 Sample configuration *65-6*

65.3 Workflow to manage residential subscribers *65-9*

65.4 Residential subscriber management *65-12*

65.5 Residential subscriber management procedures *65-22*

65.6 SAP and MSAP management *65-60*

65.7 Workflow to manage MSAPs *65-64*

65.8 SAP managment procedures *65-65*

65.1 Residential subscriber overview

The emergence of residential broadband networks and the availability of multiple service offerings, such as triple play applications create a requirement for greater service differentiation and control at the level of the individual service recipient. The 5620 SAM provides functionality for the efficient provisioning of access, QoS, and security features on IES, VPLS, and VPRN for residential subscribers, while service-level customization for end users is available using systems such as the Alcatel-Lucent 5750 SSC.

In the context of the 5620 SAM, a residential subscriber, sometimes called a subscriber, is a unique identifier that associates a group of end-user devices with policies. A subscriber can be associated with multiple SAPs on multiple NEs, and a customer can be associated with multiple subscribers.

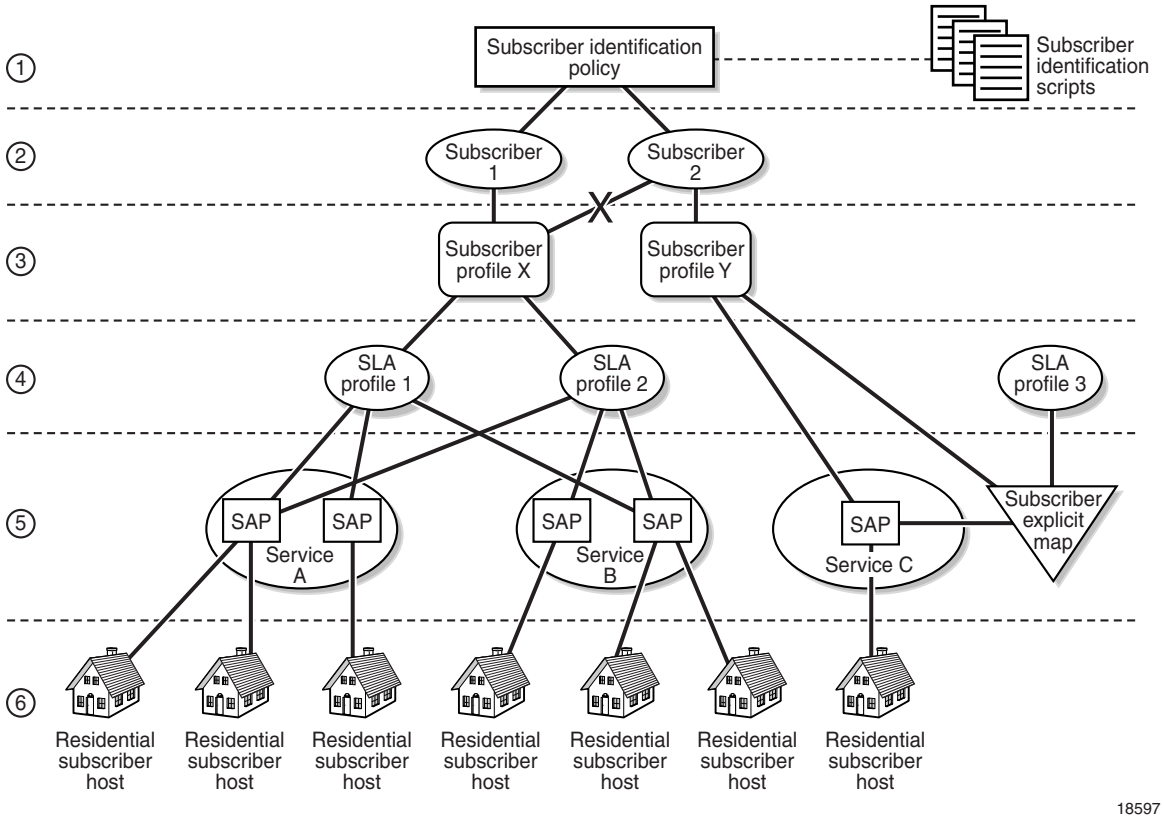
A subscriber host, sometimes called a host, is an end-user device, such as a computer, VoIP telephone, or set-top box, that connects to the provider network and receives the service traffic. Hosts with the same subscriber identifier share overall HQoS and accounting characteristics as defined in a customer SLA, but may use QoS policies and queues that differ by the type and class of service offering.

Residential subscriber management, also called enhanced subscriber management, supports service delivery models in a routed or bridged configuration, such as one VLAN per host, one VLAN per application, one VLAN for all applications, and one VLAN per service provider per application.

Residential subscriber components

Figure 65-1 shows a conceptual model of the main component relationships in residential subscriber management. The model does not represent a specific type of service or service delivery mechanism and does not show all possible component configurations.

Figure 65-1 Residential subscriber management component relationships



As shown in Figure 65-1, there is a one-to-one relationship between a subscriber and a subscriber profile and a many-to-many relationship between subscriber profiles and SLA profiles. A subscriber profile or an SLA profile can apply to multiple SAPs or NEs, and can be specified as the default profile for the SAP or the NE.

Table 65-1 lists where to find configuration information for the components shown in Figure 65-1. The numbered levels segregate components for clarity only.

Table 65-1 Residential subscriber management components

Level	Component	Description	For more information, see	Procedure
1	Subscriber identification policy	Associates a dynamic host with a subscriber	"Subscriber identification policies" in Chapter 54	54-1
	Subscriber identification script	Parses DHCP Option 82 field to extract subscriber identification for a host, and optional profile, ANCP, and intermediate destination identification strings.	"Subscriber identification policies" in Chapter 54	65-21
2	Subscriber	Unique identifier that associates a group of subscriber hosts with policies	"Residential subscriber overview" in this chapter	65-14

(1 of 2)

Level	Component	Description	For more information, see	Procedure
2	Subscriber instance	An instantiation of a subscriber on an NE	"Residential subscriber overview" in this chapter	65-15
3	Subscriber profile	Names existing ingress and egress scheduler policies and an accounting policy for use by all hosts of a subscriber	"Subscriber profiles" in Chapter 54	54-18
4	SLA profile	Names existing QoS policies to define the traffic shaping for different classes of service within an application such as HSI, VoIP, VoD, or BTV Names existing ACL policies to filter the ingress and egress traffic	"SLA profiles" in Chapter 54	54-17
5	Subscriber explicit map	Lists subscriber identifiers and the associated SLA and subscriber profiles	"Subscriber explicit maps" in Chapter 54	54-19
6	Residential subscriber host (static)	A device such as a computer or set-top box that receives service traffic using a fixed IP address	"Static hosts and residential subscriber management" in this section	65-25 68-36, 70-41, and 71-43 access interface anti-spoofing configuration steps
	Residential subscriber host (dynamic)	A device such as a computer or set-top box that receives the service traffic using a temporarily assigned IP address	"Subscriber identification policies", "Subscriber profiles", "SLA profiles", "Subscriber explicit maps", Managed SAP (MSAP), and "PPPoE policies" in Chapter 54	65-38
7	Local DHCP server and PPPoE group interface	A local user database is created and associated to a local DHCP server and PPPoE group interface configuration	"Local DHCP server" in this section	54-3 65-5 71-1 70-12

(2 of 2)

The 5620 SAM treats residential subscriber management components like policies. Depending on the distribution mode configuration of a local instance, when you modify a global component using the 5620 SAM, all local instances of the residential subscriber management component on the associated NEs can be updated. The Local Definitions tab of a component management form lists the local instances of the component.



Note — You cannot delete an active component of a residential subscriber management configuration.

Residential subscriber component and policy deployment

Global residential subscriber management components are created in draft mode. This allows operators to verify the configuration before they distribute it to the network elements. See chapter 42 for information about global and local policy instances and policy distribution modes.

The 5620 SAM deploys the components associated with a subscriber, such as policies and profiles, to an NE when one of the following occurs:

- The deployment of a subscriber identification policy with profile specifications
- The provisioning of the first static host for the subscriber on a SAP
- The provisioning of a capture SAP with an MSAP Policy to automatically create an MSAP; see Managed SAP (MSAP) for more information

After the 5620 SAM deploys the subscriber and SLA profiles, the NE creates the queues, ACL filters and HQoS schedulers specified in the profiles. The NE ignores pre-existing queue or ACL filter policies on a SAP when subscriber management is enabled on the SAP.

Subscriber identification strings

The 5620 SAM identifies the subscriber for a dynamic host by obtaining a subscriber identification string from a source such as the following:

- information that the host passes in the Option 82 field of a DHCP packet
- a RADIUS server
- the local user database

A static host requires explicit provisioning on the 5620 SAM that includes the association of a subscriber identification string.

You can optionally specify a default subscriber identification string for a SAP. You can enter the string or configure the 5620 SAM to use the SAP ID as the string.

Obtaining subscriber identification strings from DHCP packets

When a dynamic residential subscriber host requests an IP address using DHCP, the host can include a subscriber ID string and optional profile ID strings in the Option 82 field of the DHCP packet. If the request is approved by a DHCP server, the NE obtains the subscriber ID string for the host from the Option 82 information in the returning ACK message. The subscriber ID string is a match criterion for the assignment of SLA and subscriber profiles to the host unless profile ID strings are explicitly encoded in the DHCP option information by the host or configured as SAP default profiles. You can also configure a default subscriber ID string on a SAP.



Note — If adding Option 82 information to a DHCP relay packet causes the packet to exceed the DHCP relay maximum of 1500 bytes, the NE forwards the DHCP request without the Option 82 information. For this reason, short strings can be used as aliases for profile names.

Migrating to the TPSDA model

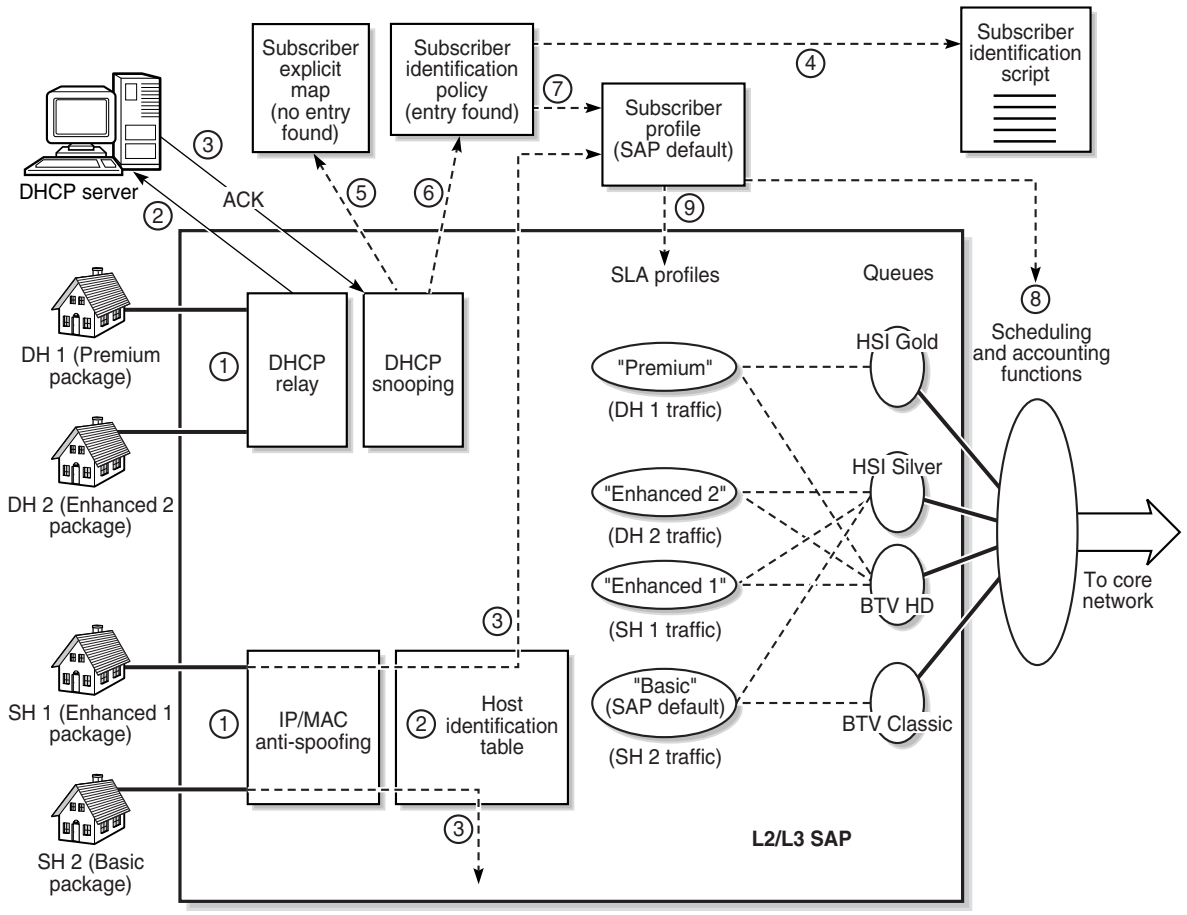
The 5620 SAM facilitates the migration of hosts from SAP-based aggregation to the TPSDA model. You can use residential subscriber managment functions to:

- Associate a subscriber with a SAP by using the SAP identifier as the subscriber identification string. The existing hosts on a SAP can then be automatically associated with a subscriber.
- Rename a subscriber. This changes the subscriber identification string for all hosts and facilitates a move from a default subscriber identification string to a string that complies with a particular naming scheme.
- Configure an intermediate destination identifier, such as a DSLAM name, for a static host and obtain the identifier from the Option 82 information in a DHCP packet. This functionality enables the listing of the hosts for a specific DSLAM and facilitates interworking with other TISPAN components such as the 5750 SSC.
- Configure a default subscriber identification string for the hosts on a SAP. This enables residential subscriber management functionality without the use of a subscriber identification policy or RADIUS authentication. This default string is associated with hosts when a string is not available from another source.
- Interpret an SLA profile string or subscriber profile string from a host as the profile name when a profile with a matching profile string is not found. This eliminates the need to map a profile string to a profile.

65.2 Sample configuration

Figure 65-2 shows how residential subscriber management assigns resources to dynamic and static hosts. Many different configurations are possible; the sample portrays the residential subscriber management mechanism rather than a particular service delivery model. For simplicity, the sample consists of one subscriber instance on one SAP, and two types of service offering. Each service offering is available in two classes.

Figure 65-2 Sample configuration



The customer provides a subscriber identification string, the names of the four end-user service packages, and the bandwidth and class requirements for each package. Each package is a combination of HSI and BTV. A 5620 SAM operator creates four queues and four SLA profiles with which the queues are associated, as shown in Table 65-2. Alcatel-Lucent recommends that the 5620 SAM operator give the SLA profiles the same names as the packages to prevent confusion.

Table 65-2 Sample configuration service packages

Subscriber host	Package name	SLA profile name	Associated queues
DH 1	Premium	Premium	HSI Gold, BTV HD
DH 2	Enhanced 2	Enhanced 2	HSI Silver, BTV HD

(1 of 2)

Subscriber host	Package name	SLA profile name	Associated queues
SH 1	Enhanced 1	Enhanced 1	HSI Gold, BTV Classic
SH 2	Basic	Basic	HSI Silver, BTV Classic

(2 of 2)

The customer offers two classes of BTV and HSI services:

- BTV HD: high-definition broadcast television
- BTV Classic: regular-definition broadcast television
- HSI Gold: high-bandwidth broadband Internet access
- HSI Silver: regular broadband Internet access

The following steps, which correspond to the numeric labels in the upper part of Figure 65-2, define the sequence of events for dynamic subscriber hosts that attempt to join the network.

1 Dynamic Host 1 (DH 2) and Dynamic Host 2 (DH 2) each send a DHCP request to the SAP.

2 DHCP relay on the SAP forwards the DHCP requests to the DHCP server.

3 The DHCP server authorizes the requests and responds with a DHCP ACK message for each subscriber host.

4 The subscriber identification policy uses a script to obtain the subscriber identification string, an optional subscriber profile string, and an optional SLA profile string from the Option 82 information in each ACK message. DH 1 and DH 2 provide the same subscriber profile identification string but different SLA profile strings.

5 The NE checks the subscriber identification string values against the entries in the subscriber explicit map and finds no matching entries for the hosts.

6 The NE checks the subscriber profile string and the SLA profile string values for each host against the subscriber identification policy.

7 The NE assigns the same subscriber profile to DH 1 and DH 2 based on the subscriber profile string provided by each host.

8 DH 1 is the first host to join the network, so the scheduling and accounting functions associated with the assigned subscriber profile are instantiated on the SAP.

9 The NE matches the SLA profile string provided by each host to an SLA profile. The NE assigns the Premium SLA profile to DH 1 and the Enhanced 2 SLA profile to DH 2 based on the provided SLA profile strings. These are the first hosts of the subscriber to join the network, so the appropriate queues are instantiated on the SAP based on the SLA profile specifications, and host traffic subsequently flows.

The following steps, which correspond to the numeric labels in the lower part of Figure 65-2, define the sequence of operations for static subscriber hosts that join the network.

1 Static Host 1 (SH 1) turns on the computer, and Static Host 2 (SH 2) turns on the television.

2 The host devices request network access; IP- matching (and optional MAC-matching) anti-spoofing on the SAP checks the static host table on the NE and validates both requests.

3 The NE assigns resources to each static host based on subscriber profile and SLA profile designations, and host traffic subsequently flows.

- The static host table entry for SH1 names a subscriber profile and an SLA profile. Although SH 1 is the first host to use this SLA profile, the queues defined in the profile are already instantiated because of the application of the SLA profiles for DH 1 and DH 2.
- For SH 2, there is no explicit association between the host and a subscriber profile or an SLA profile, so the NE assigns the SAP default subscriber and SLA profiles, which define the most basic service package the customer offers to end users.

65.3 Workflow to manage residential subscribers

1 Create a service that effectively delivers the proposed residential service offering; see Chapter 61.

2 Depending on your service delivery model, configure the following policies as required:

a subscriber identification policy. See Procedure 54-1.

b ANCP policy. See Procedure 54-2.

c PPPoE policy. See Procedure 54-3.

d PPP policy. See Procedure 54-4.

e MSAP policy. See Procedure 54-5

f host tracking policy. See Procedure 54-6.

g category map policy. See Procedure 54-7.

h credit control policy. See Procedure 54-8

i IGMP policy. See Procedure 54-9.

j BGP Peering policy. See Procedure 54-10.

k diameter policy. See Procedure 54-11.

l subscriber multicast CAC policy. See Procedure 54-12.

m mobile gateway profile. See Procedure 54-13.

n host lockout policy. See Procedure 54-14.

o RADIUS script policy. See Procedure 54-16.

See Chapter 54 for more information about policies related to residential subscribers.

3 Create ingress and egress scheduler policies for the subscriber hosts in accordance with the customer SLA; see Procedure 43-15.

4 Create an accounting policy for the customer; see the *5620 SAM Statistics Management Guide*.

5 Create access ingress and access egress QoS policies for the different applications, for example, HSI and VoIP, and levels of service, for example, gold, silver, and bronze, that subscriber hosts are to receive. See Procedures 43-1 and 43-3. Associate the queues in the QoS policies with the previously created ingress and egress scheduler policies.

6 Specify a unique subscriber identification string for the subscriber, according to your customer specifications. See "Residential subscriber components" in this chapter for the different options for specifying a subscriber identification string.

7 Create a RADIUS-based accounting policy for the subscriber, as required; see Procedure 49-1.

8 Create a policer control policy for the subscriber, as required; see Procedure 43-20.

9 Create SLA profiles that name the previously created QoS policies; see Procedure 54-17.

- **i** Create a different SLA profile for each class of service offering.
- **ii** Use override values to customize the policy values, as required.
- **iii** Use override values to customize the policer values, as required.

10 Create a subscriber profile; see Procedure 54-18.

- **i** Choose the previously created ingress and egress scheduler policies.
- **ii** Choose the previously created accounting policy.
- **iii** Enable accounting.
- **iv** Assign the previously created RADIUS-based accounting policy, as required.
- **v** Assign the previously created ingress and egress policer control policies, as required.
- **vi** Associate one or more of the previously created SLA profiles with the subscriber profile.

11 Create, configure, and manage SAPs, as required.

- **a** Enable automatic generation of subscriber IDs; see Procedure 65-1.
- **b** Assign the subscriber profile and SLA profiles to the service SAP;. see Procedure 65-23.
- **c** Enable or disable residential subscriber management on a SAP; see Procedure 65-24.
- **d** Specify a subscriber identifier, subscriber profile, and SLA profile for each static host, as required, if default values are not configured on the SAP; see Procedure 65-25 for more information.

e Configure a MEP on a SAP; see Procedure 65-26.

f List and manage subscriber management SAPs; see Procedure 65-27.

12 Create, configure, and manage MSAPs, as required.

a Create a capture SAP that will enable the creation of an MSAP; see Procedure 65-28.

b List MSAPs and view MSAP properties; see Procedure 65-29.

c View an MSAP event log, modify the global MSAP log policy, and purge MSAP log records; see Procedure 65-30.

d Modify and re-evaluate an MSAP policy on an MSAP; see Procedure 65-31.

e Modify an MSAP policy and re-evaluate the MSAPs; see Procedure 65-32.

f Delete an MSAP; see Procedure 65-34.

g Delete an MSAP policy; see Procedure 65-35.

13 Configure or monitor DHCP or NE SHCV events or databases, as required.

a Configure DHCP event monitoring for a SAP; see Procedure 65-36.

b Monitor DHCP events for a SAP; see Procedure 65-37.

c Configure DHCP lease management for a subscriber host; see Procedure 65-2.

d Configure DHCP event monitoring for a subscriber host; see Procedure 65-3.

e Monitor DHCP events for a subscriber host; see Procedure 65-4.

f Configure a local user database to authenticate DHCP clients; see Procedure 65-5.

g Configure NE SHCV event handling; see Procedure 65-7.

14 Turn up the service.

15 Provide the customer with the necessary IP information for provisioning dynamic and static hosts in the customer network.

16 Perform one or more of the following, as required.

a Create a subscriber explicit map, if required; see Procedure 54-19.

b Retrieve PPPoA sessions; see Procedure 65-8.

c Configure a MEP on an SDP Binding; see Procedure 65-9.

d Configure L2Aware static port forwarding on a residential subscriber instance; see Procedure 65-10.

e Resynchronize static port forwarding entries; see Procedure 65-11.

f Collect, view, and clear host tracking statistics and information; see Procedure 65-12.

17 View information associated with the residential subscriber, as required.

a View subscriber host information; see Procedure 65-13.

b View a subscriber and the associated subscriber hosts; see Procedure 65-14.

c View a subscriber instance and the associated subscriber hosts; see Procedure 65-15.

d View or configure active residential subscriber hosts on a SAP; see Procedure 65-38.

e View subscriber DHCP lease information; see Procedure 65-16.

f View SHCV log events; see Procedure 65-18.

g View SLA profile instances on residential subscriber instances; see Procedure 65-17.

18 Modify a subscriber's subscription details, as required.

a Rename a subscriber; see Procedure 65-19.

b Reset a subscriber's subscription credit limit; see Procedure 65-20.

c Modify the primary subscriber identification script or URL; see Procedure 65-21.

d Delete an inactive residential subscriber instance; see Procedure 65-22.

65.4 Residential subscriber management

The 5620 SAM supports the creation and configuration of residential subscriber management components using configuration forms. Configuring residential subscriber management on the 5620 SAM involves the creation and configuration of the following components, depending on the service delivery model:

- subscriber identification policies
- subscriber profiles
- SLA profiles
- subscriber explicit map entries
- ANCP policies
- PPPoE policies
- MSAP policies
- host tracking policies
- category map policies
- credit control policies
- IGMP policies
- BGP peering policies
- diameter policies
- subscriber multicast CAC policies
- mobile gateway profiles
- host lockout policies
- RADIUS script policies

For detailed NE-specific information about residential subscriber management, see the enhanced subscriber management sections of the *7450 ESS OS Triple Play Guide* and the *7750 SR OS Triple Play Guide*. For information about configuring residential subscriber policies and profiles, see Chapter 54.

A host requires subscriber-profile and SLA-profile associations to gain access to the network. Profiles define service attributes for hosts such as scheduling, accounting, security, and traffic prioritization by application type. A profile uses existing 5620 SAM policy definitions and allows the customization of policy parameters using override values.

A 5620 SAM user who is assigned the administrator, subscriber management, service management, or policy management scope of command role can perform all residential subscriber management functions, such as managing profile or DHCP-lease information.

The 5620 SAM allows the configuration of multiple components in one operation, but limits configuration to those parameters that are not specific to a component. For example, when a policy is applied to multiple profiles, the 5620 SAM removes pre-existing policy override values in the profiles.

Configuration requirements

The following must be true before you can enable residential subscriber management on a SAP or deploy a profile to an NE.

- The NE must be a 7450 ESS, 7750 SR, or 7710 SR.
- For dynamic hosts on the SAP:
  - DHCP snooping is enabled on the upstream SAP or SDP.
  - For IES, DHCP relay is enabled on the downstream SAP.
- The NE has sufficient resources for creating the SLA profile instances, queues, and schedulers.
- For new or existing static hosts on the SAP:
  - Anti-spoofing on the SAP is configured with at least IP matching criteria.
  - A subscriber identification string is assigned.
  - A subscriber profile is assigned.
  - An SLA profile is assigned.
  - An IP address is assigned.

Local DHCP server

A local DHCP server leases IP addresses to clients in the network. Options are configured to define the IP address properties, such as, the length of time an IP address is active and which DNS server must be used. A local user database is used to authenticate and authorize clients requesting IP addresses from the local DHCP server. If the local DHCP server does not use the local user database, the server can use the GI address to assign free IP addresses, however it is not possible to configure match or authentication parameters.

Three applications are targeted for the local DHCP server.

- Subscriber aggregation using a single NE or TPSDA.
- Business services running VPRN and locally attached to the host can request and obtain IP addresses directly from the server.
- The DHCP server identifies an IP request from a PPPoE client and provides an IP address and options.

DHCP servers can be integrated with Enhanced Subscriber Management for DHCP and PPPoE clients. A local DHCP server can be created in the routing instance window or VPRN service site window. A local DHCP server created in the VPRN service site can be associated with the L3 access interface on a VPRN service only. A local DHCP server created in the routing instance window can be associated with a network interface or L3 access interface on an IES.

Failover support

You can configure failover support on local DHCPv4 and DHCPv6 servers. The same IPv6 prefix or IPv4 address range can be shared between the two peering DHCP servers in a redundant configuration. Either DHCP server can allocate a new lease from the same address range or prefix. To avoid IP address duplication, a single active path is available from the clients to one of the DHCP servers in a redundant configuration. The single active path is ensured through a protection mechanism in a dual homed environment in the access side of the network. The supported protection mechanisms are SRRP or MC-LAG.

Local user database

A local user database is configured and associated with the local DHCP server to provide local authentication. The local DHCP server must have a pool of IP addresses configured, otherwise it is not able to lease IP addresses.

A create local user database configuration form is available from the Manage Residential Subscribers form. See Procedure 65-5 for more information about configuring a local user database. Once a local user database is configured, it can be associated with a local DHCP server and PPPoE configuration on a group interface.

When a local user database is not configured, you can use GI addresses to access free IP addresses, however the clients requesting the IP address will not be authenticated.

ARP host

You can use the 5620 SAM to configure and retrieve ARP hosts on a 7750 SR. ARP hosts are a subtype of enhanced subscriber host objects. The creation of the object is triggered by the reception of ARP messages from end-user devices. ARP hosts can be configured as an alternative to DHCP subscriber hosts or PPPoE sessions.

ARP host configuration can be performed on VPLS and MVPLS L2 access interfaces, IES and VPRN group interfaces, and VPRN retailer subscriber interfaces. The configuration includes enabling the functionality, setting the maximum limit of hosts per SAP or interface, and setting the default authentication interval.The configuration must be performed in conjunction with other enhanced subscriber management configuration on these interfaces. ARP hosts can be retrieved from the VPLS, MVPLS, and IES or VPRN SAPs. ARP hosts can also reside on MSAPs.

You can retrieve ARP hosts from the Manage→Residential Subscribers menu option. See Procedure 65-13 for more information about the persistence and retrieval of subscriber hosts.

Static hosts and residential subscriber management

Static subscriber hosts require explicit provisioning rather than an association with a subscriber identification policy. Static hosts for VPLS are configurable on the anti-spoofing tab of the L2 access interface management form. For IES and VPRN services, static hosts are configurable using the management form for a SAP on a group interface. Static host configuration involves the following elements:

- IP address
- MAC address (optional)
- subscriber ID string, or the use of the SAP ID as the subscriber ID
- valid subscriber profile
- valid SLA profile
- ANCP string
- intermediate destination, such as a DSLAM
- application profile



Note — When residential subscriber management is enabled on a VPLS SAP that is part of an operational MC ring group, the following must be configured on each static host:

- an intermediate destination that is a ring node in the MC ring group
- subscriber identification, such as a subscriber ID string or the use of the SAP ID as the subscriber ID
- a subscriber profile
- an SLA profile

Subscriber host connectivity verification

Aside from relatively infrequent IP-address lease renewal, DHCP has no session-monitoring or connection-monitoring capability. Residential subscriber management provides this functionality for DHCP hosts and static hosts using subscriber host connectivity verification, or SHCV.

When SHCV is enabled on a SAP, an NE issues a periodic ARP request to each host on the SAP. If the NE receives no reply to an ARP request within the specified interval, the NE raises an event. When SHCV is configured to drop a lost host, the NE immediately removes the host from its active subscriber host table.

SHCV records the state information that it collects for hosts on a SAP and maintains a history of connectivity-related events for troubleshooting purposes. The size of the history log is restricted by a size-constraint policy.

SHCV operates in conjunction with DHCP snooping and is configurable on VPLS, VPRN, and IES SAPs and on IES group interfaces. Because it uses ARP, SHCV automatically populates the FIBs of bridging devices in the access and provider networks. The configurable items for SHCV on a SAP include:

- frequency of connectivity checks
- source of the ARP request
- action to take when a host loses connectivity



Note — On an L2 access interface, SHCV uses the NE system IP address as the source of the ARP request. On an L3 access interface, SHCV uses the IP- and MAC-address combination of the interface or the VRRP state for the interface as the ARP source. On IES group interfaces, SHCV uses the address of the subscriber interface as the source.

The behavior that an NE exhibits toward SHCV events is configurable using the residential subscriber management form. The configurable NE SHCV items include:

- maximum host connectivity loss rate
- action to take when the connectivity loss rate exceeds the maximum
- action to take when the NE drops an event trap, as such an event may indicate a high connectivity loss rate

SHCV event handling on an NE is disabled by default. When SHCV is enabled on a SAP but is disabled on the NE, the 5620 SAM records the blocking of SHCV events in the SHCV log. This ensures that an operator is aware of SHCV activity when viewing the SHCV log, even if the NE is configured to suppress SHCV events.

The following conditions represent an SHCV host connectivity loss:

- absence of a host response
- inconsistency between the reply data and the DHCP lease state

An NE makes more than one SHCV attempt before it raises an event against a host to ensure that the absence of a host response indicates a host connectivity problem and is not simply the result of occasional packet loss.

When a SAP becomes operationally down, the NE generates one trap for the SAP rather than one trap for each host on the SAP. When the SAP returns to service, the NE forwards a trap for each host as it verifies the restoration of connectivity. SHCV generates the following event traps:

- SAP up
- SAP down
- host up
- host down
- trap dropped

Routed CO

A broadband access network typically requires the aggregation of the traffic from access equipment before routing of the traffic is possible. Routed CO functionality allows a network operator to directly connect a DSLAM or similar multiplexer to a router such as the 7750 SR. Residential subscriber management, combined with the use of DSCP or dot1p values, supports access-integration models such as the following:

- one SAP for all subscribers and service offerings
- one SAP per service offering
- one SAP per subscriber

Routed CO allows the configuration of subscriber interfaces and group interfaces on IES and VPRN. A subscriber interface defines the subnets that are available to a subscriber. A group interface is a child object of a subscriber interface that allows the configuration of multiple SAPs as part of a single interface. Routed CO functionality depends on residential subscriber management to maintain the subscriber host information.

There is no direct association between the subnets and the group interfaces. Subnets can be shared between group interfaces. If the host IP address is not in one of the subnets, packets from the network to that host IP are not received by the subscriber or group interfaces.

A subscriber interface defines a maximum of 16 subscriber subnets and acts as the DHCP relay agent for a subscriber. For the forwarding of DHCP packets to a subscriber server, a subscriber interface requires the specification of a gateway address that is in one of the subscriber subnets. Group interfaces below the subscriber interface inherit this gateway address but can specify an override value if required.

All SAPs in a group interface use the same port. The first SAP on a group interface determines which port the group interface uses. Additional SAPs for the group interface must be associated with the group-interface port during SAP creation.

A group interface is similar to a regular IES interface except for the following.

- Multiple SAPs are configurable.
- No IP addresses are specified.
- No broadcast traffic is permitted.
- No loopback mode exists.
- No static ARP can be specified.
- VRRP is not supported.

When a subscriber interface or a group interface is operationally disabled, no packets are sent to or from the subscriber hosts on the SAPs of the interface, but the state information for a static or dynamic host persists until the static host is removed from the NE by an operator or the DHCP lease of the dynamic host expires.

Because the configuration of multiple SAPs on a group interface makes normal forwarding of DHCP responses to hosts impossible, DHCP relay for routed CO maintains a cache of DHCP requests. If a DHCP server response does not arrive within the specified interval time, the NE discards the cache entry. The 5620 SAM operator can choose to have the NE use the Option 82 circuit ID field in a DHCP request as the match criterion for the returning DHCP ACK message.

You can configure NAT for dynamic subscriber hosts in a routed CO deployment. NAT for routed CO requires a NAT policy that is associated with a subscriber profile. In an IES routed CO deployment, NAT is configured on the base routing instance of an NE. In a VPRN routed CO deployment, NAT is configured on the VPRN routing instance. See chapter 24 for information about configuring and deploying NAT, and about configuring a NAT policy. See Procedure 54-18 for information about associating a NAT policy with a subscriber profile.

Lease populate is enabled on a group interface by default, and the number of allowable lease entries is set to one. All SAPs on the group interface inherit this configuration during creation.

See chapters 70 and 71 for more information on configuring subscriber and group interfaces for IES and VPRN services.

Wholesale and retail configurations for VPRN services

A VPRN routed CO allows a service provider to resell wholesale carrier services while providing direct DSLAM connectivity. You can create a VPRN service for the retailer and also define subscriber access and configuration information for the retailer network. The implementation of configuration changes occurs as if the VPRN is a standalone router using the routed CO model. The benefit of this model is flexibility for the retailer and decreased involvement for the wholesaler.

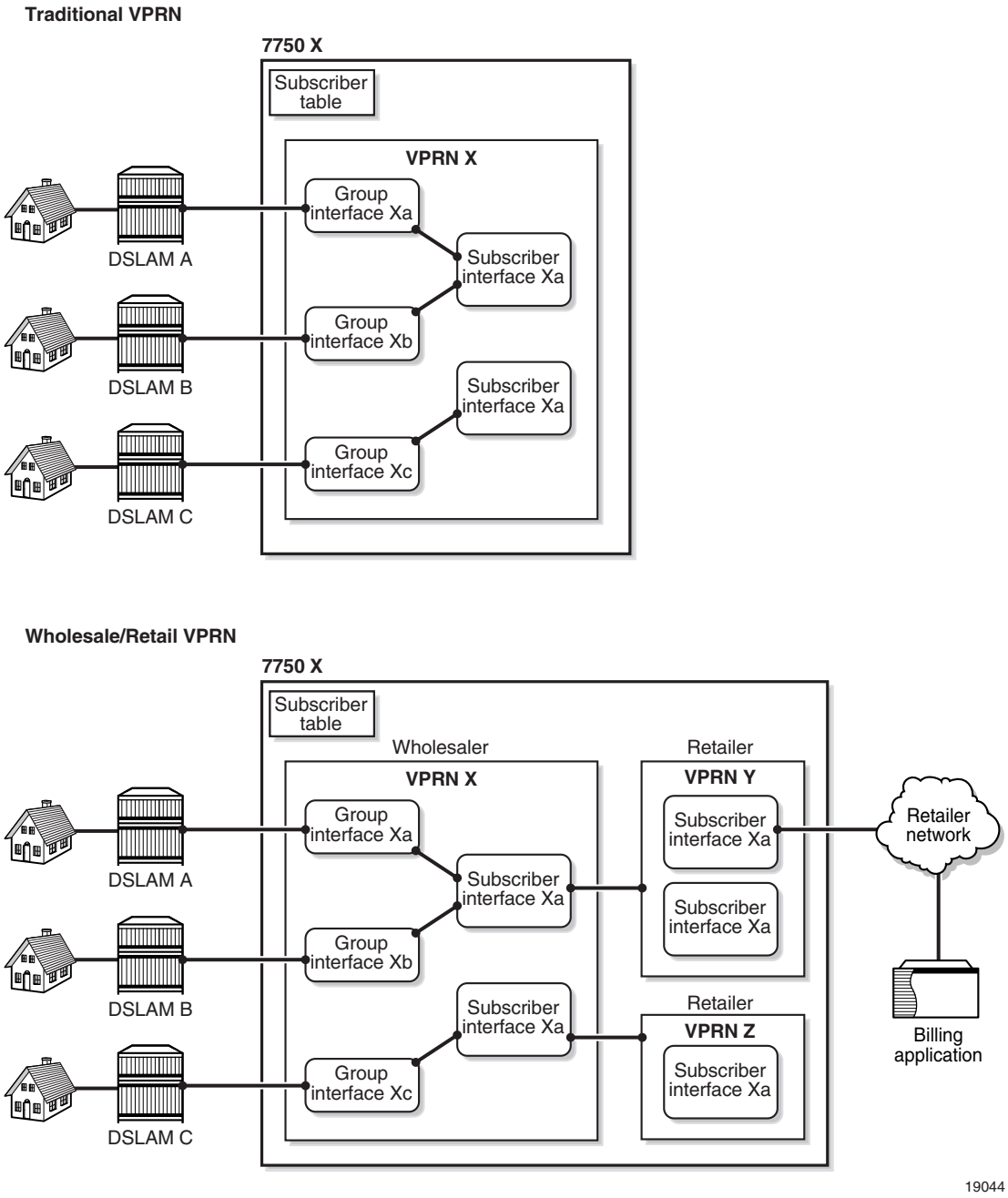
You must use a subscriber SAP to support shared access for multiple retailers. Another dependency of shared access is the requirement for the wholesaler to maintain separate access nodes for each retailer with network scaling issues.

In the wholesale and retail model, the wholesaler instance connections that are common to the access nodes are distributed to many retail instances. Upstream subscriber traffic ingresses into the wholesaler instance and, after identification, is then forwarded into the retail instance. The reverse principle occurs for traffic in the opposite direction. The wholesale and retail traffic flow is controlled with minimal communication to the RADIUS server. A RADIUS policy is defined in the wholesaler instance. The RADIUS response used during the subscriber instantiation provides the service context of the retailer VPRN. If the wholesaler has a retail business, the operator can configure a separate VPRN for their retail services.

The retailer subscriber interface primarily controls the DHCP configuration. The single exception to this model is the lease-populate value. The lease-populate value in the wholesale context controls the individual SAP limits. The lease-populate value in the retail subscriber interface controls the limits for that retailer interface. The wholesale and retail limits must be met before the instantiation of a new subscriber.

Figure 65-3 shows the configuration for a traditional and wholesale retail VPRN.

Figure 65-3 Routed CO for traditional and wholesale/retail VPRNs



See chapter 71 for more information on configuring the forwarding service component for wholesale and retail VPRN services.

Subscriber host polling and monitoring

Subscriber hosts can be periodically polled and monitored for certain DHCP event changes. A subscriber host monitoring configuration form is available from the Manage Residential Subscribers form.

The maximum number of hosts that can be selected for monitoring is configurable through XML; the default is five. Host monitoring has a performance impact, so only a small number are typically monitored at one time.

The Monitored Subscriber Host form displays a variety of polled information about the host that is obtained from the NE. You can also open a DHCP event log for the host from the Host Properties form. The logged events include information on DHCP lease renewals, lease expiration, and profile changes. An entry is added to the table whenever a new event occurs. You can purge event entries using the Host Properties form.

Host monitoring can be started, stopped, or removed from the monitoring configuration form, and the monitoring period and polling interval can be configured.

The Host monitored objects and associated events are stored in the 5620 SAM database. The monitoring continues until the monitoring period elapses or the monitoring is stopped by a 5620 SAM operator.

Subscriber services

The 5620 SAM supports the retrieval of subscriber services and related attributes from PPP or IPoE subscriber hosts. A subscriber service specifies a mode of operation in which a subscriber-specific service is activated and deactivated on a PPPoE session via a RADIUS Access-Accept message or a CoA-Request message. This function is sometimes referred to as Radius Based Policy control, or RaBaPol. For information on retrieving subscriber services from subscriber hosts, refer to Procedure 65-13.

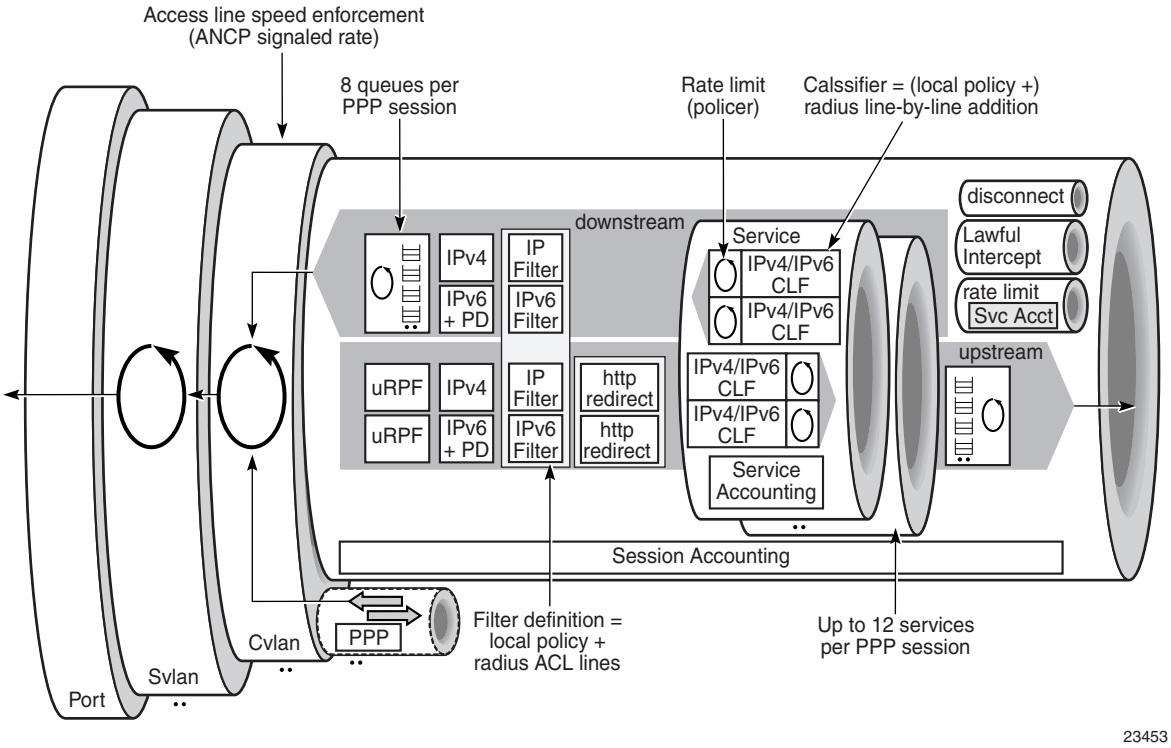
Single or multiple subscriber service activation and/or deactivation calls can be included in Access-Accept messages for new PPPoE sessions, or in CoA-Request messages for existing PPPoE sessions. PPPoE sessions can be IPv4, IPv6 or dual stack. Subscriber services can also operate on the PPPoE session itself.

Examples of subscriber services are:

- apply or change the dynamic bandwidth of a PPPoE session
- apply or change a QoS profile
- activate or deactivate HTTP redirection
- apply or change a rate-limiting service
- a Disconnect Request for a PPPoE session

Figure 65-4 shows the subscriber service RaBaPol model.

Figure 65-4 Subscriber services model



Managed routes

The 5620 SAM can retrieve managed route (also known as framed route) information from the NE for hosts instantiated on IES and VPRN services. A routed subscriber host is a subscriber with subnets behind the routed gateway in order to support subscriber hosts with regular routers. The subscriber host associated subnets are learned through RADIUS VSAs (up to 16 routes).

Framed routes (IPv4 subnets) are displayed on the following ESM session types:

- DHCP lease
- ARP host
- PPP session

Framed IPv6 routes (IPv6 prefixes) are displayed on the following ESM session types:

- DHCPv6 lease
- PPP DHCPv6 session
- PPP SLAAC session
- IPoE SLAAC host (displayed within the subscriber host object)

65.5 Residential subscriber management procedures

Use the following procedures to perform residential subscriber management tasks.

Procedure 65-1 To enable automatic generation of subscriber IDs

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Auto Subscriber ID Key (Residential Subscribers) from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of managed network elements appears.

4 Select a managed network element from the list and click on the Properties button. The Auto Subscriber ID Key (Edit) form opens.

5 As required, disable the Default parameter and configure the following parameters in the PPP Subscriber ID Key panel:

- PPP Key 1
- PPP Key 2
- PPP Key 3
- PPP Key 4
- PPP Key 5

6 As required, disable the Default parameter and configure the following parameters in the IPoE Subscriber ID Key panel:

- IPoE Key 1
- IPoE Key 2
- IPoE Key 3
- IPoE Key 4

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The Auto Subscriber ID Key (Edit) form closes.

9 Close the Manage Residential Subscribers form.

Procedure 65-2 To configure DHCP lease management for a subscriber host

DHCP is used to assign IP addresses to hosts or workstations on the network. This function is usually performed by a DHCP server. Essentially, it “leases” out addresses for specific times to the various hosts. If a host does not use a specific address for a set period of time, that IP address can then be assigned to another machine by the DHCP server.

In order to allow the DHCP client to lease out address for specific times, the 5620 SAM allows an operator to force the DHCP client to change its state by sending a renewal command. Upon receipt of the renewal command from the 5620 SAM, the DHCP client changes to the renewal state and then negotiates with the DHCP server for lease times.

Conversely, an operator can also terminate (clear) a lease for a particular host from within the Residential Subscriber Host form of 5620 SAM.



Note — The DHCP lease renewal and termination are supported only on dynamic hosts, not on static hosts or subscriber hosts.

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Select Residential Subscriber Host from the object drop-down list.

3 Click on the Select buttons to specify the site, service ID, and service access point for which you want to view subscriber host information.

4 Configure the Inner Encapsulation Value and Outer Encapsulation Value parameters.

The Outer Encapsulation Value parameter is configurable only when the port encapsulation type is Dot1 Q or Q in Q. The Inner Encapsulation Value parameter is configurable only when the port encapsulation type is Q in Q.

5 Click on the Search button. A list of subscriber hosts is displayed.

6 Select one or more entries in the list.



Note — You can renew a lease for multiple entries. However, you can perform a lease termination for only one host at a time.

7 Perform one of the following steps.

a To renew the lease, click on the Force Renew button.

b To terminate the lease, click on the Clear Lease State button.

8 A dialog box appears. Click on the Yes button. The action is completed.

9 Close the Manage Residential Subscribers form.

Procedure 65-3 To configure DHCP event monitoring for a subscriber host

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Residential Subscriber Hosts from the object drop-down list.

3 Click on the Select buttons to specify the site, service ID, and service access point for which you want to view subscriber host information.

4 Configure the Inner Encapsulation Value and Outer Encapsulation Value parameters.

The Outer Encapsulation Value parameter is configurable only when the port encapsulation type is Dot1 Q or Q in Q. The Inner Encapsulation Value parameter is configurable only when the port encapsulation type is Q in Q.

5 Click on the Search button. A list of subscriber hosts appears.

6 To configure DHCP monitoring for a particular subscriber host, select the entry from the list and click on the Create Monitored Host button. The Monitored Subscriber Host form opens.



Note — A maximum of five hosts or five SAPs can be monitored simultaneously. If more than the maximum number of hosts is selected and configured for monitoring an error message will be displayed.

7 Configure the parameters:

- Monitoring Period
- Units
- Polling Interval

8 Click on the OK button to close the Monitored Subscriber Host form.



Note — You must complete Procedure 65-4 to enable and schedule subscriber host monitoring.

9 Close the Manage Residential Subscribers form.

Procedure 65-4 To monitor DHCP events for a subscriber host

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Monitored Subscriber Host from the object drop-down list.

3 Configure the filter criteria at the top right panel of the form, if required.

4 Click on the Search button. A list of monitored subscriber hosts appears.

5 To initiate or view DHCP monitoring for a particular subscriber host, select the entry from the list and click on the Properties button. The Monitored Subscriber Host (Edit) form opens with the General tab displayed.

6 You can perform one or more of the following on this form:

   a To start monitoring the chosen subscriber host, click on the Start Monitor button.

   b To stop monitoring the chosen subscriber host, click on the Stop Monitor button.

   c To remove monitoring of the chosen subscriber host, click on the Delete button.

   d To change the Monitoring Period, click on the Stop Monitor button, enter the desired value into the field, and select an appropriate Unit from the adjacent drop-down menu.

   e To change the Polling Interval, click on the Stop Monitor button and then select the desired value from the drop-down menu.

7 To view DHCP events for the chosen subscriber host, click on the Events tab. The DHCP Events list is displayed.

8 Select an event from the list and click on the Properties button to view detailed information about the event.

9 Click on the OK button to close the Monitored Subscriber Interface form.

10 Close the Manage Residential Subscribers form.

Procedure 65-5 To configure a local user database for subscriber host authentication

Perform this procedure to create or modify a local user database on a local DHCP server. A local user database can be used as an alternative to a RADIUS server to authenticate DHCP and PPP client connection attempts.

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Local User Database (Local User DB) from the object drop-down list.

3 Perform one of the following.

a Modify an existing database. Perform the following steps.

i Click on the Select button beside the Site ID parameter and choose an NE from the Select a Local User Database Capable Network Element form.

ii Click on the Search button. A list of local user databases on the specified NE is displayed.

iii Select a local user database and click on the Properties button. The Local User Database (Edit) form opens with the General tab displayed.

b Create a database. Perform the following steps.

i Click on the Create Local User Database button. The Local User Database (Create) form opens with the General tab displayed.

ii Click on the Select button in the Site panel and choose an NE from the Select a Local User Database Capable Network Element form.

iii Configure the Displayed Name parameter.

4 Configure the remaining parameters:

- Description
- Administrative State

5 Click on the tab. The Match List tab is displayed.

6 Configure the parameters:

- Match Type 1
- Match Type 2
- Match Type 3
- Match Type 4



Note — You cannot set two parameters to the same value.

7 Click on the Circuit ID Mask tab.

8 Configure the parameters:

- Circuit ID Mask Prefix String
- Circuit ID Mask Prefix Length
- Circuit ID Mask Suffix String
- Circuit ID Mask Suffix Length

9 Click on the Masks tab.

10 Click on the Create button. The Local User Database Mask form opens.

11 Configure the parameters:

- Match Type
- Prefix String
- Prefix Length
- Suffix String
- Suffix Length

12 Click on the OK button. A dialog box appears.

13 Click on the OK button. The Local User Database Mask form closes.

14 Click on the Hosts tab.

15 Click on the Create button. The Local User DB Host form opens with the General tab displayed.

16 Configure the parameters:

- Host Name
- Administrative State
- Domain Name
- Server Address

17 Click on the Select button in the Subscriber Authentication Policy panel to choose a subscriber authentication policy from the Select Subscriber Authentication Policy form.



Note — If you are using LLID pre-authentication, choose a subscriber authentication policy that is associated with the pre-authentication server.

18 Click on the Select button beside the MSAP Policy Name parameter to choose an MSAP policy from the MSAP Policy form.

19 Click on the Select button beside the MSAP Service ID parameter to choose an MSAP service ID from the Service form.

20 Perform one of the following.

a Click on the Select button beside the MSAP Group Interface Name parameter to choose a group interface from the Group Interface form.

b Manually specify a group interface. Perform the following steps.

i Type the group interface name in the MSAP Group Interface Name field.

ii If the port ID is not included in the typed name, set one of the following parameters to Port ID, depending on whether the port ID is to be the prefix or suffix of the group interface name:

- MSAP Group Interface Prefix
- MSAP Group Interface Suffix



Note — If the combined length of the port ID and the typed name exceeds 32 characters, an alarm is raised.

21 Click on the Select button beside the RADIUS Accounting Policy field to choose a RADIUS accounting policy from the Select RADIUS Accounting Policy form.

22 Click on the Select button beside the Duplicate RADIUS Accounting Policy field to choose a duplicate RADIUS accounting policy from the Select RADIUS Accounting Policy form.

23 Click on the Address tab.

24 Configure the parameters:

- IP Address
- Use Gateway Interface (GI) Address
- Pool Name/Client Pool Delimiter

25 In the IP Address Pool panel, configure the parameters:

- IP Address Pool Name
- Second IP Address Pool Name

26 In the Client Pool panel, configure the Use Pool From Client parameter.

27 In the IPv6 panel, configure the IPv6 addressing parameters, if required:

- IPv6 Address
- IPv6 Delegated Prefix (or IPv6 Prefix)
- Prefix Length
- IPv6 Delegated Prefix Length
- IPv6 Delegated Prefix Pool
- IPv6 WAN Address Pool
- IPv6 SLAAC Prefix
- Prefix Length

28 Click on the Host Identification tab.

29 Configure up to four of the following parameter groups.

- **Group 1**
  - Circuit ID Format
  - Circuit ID
- **Group 2**
  - MAC Address
  - Option 60
- **Group 3**
  - Remote ID Format
  - Remote ID
- **Group 4**
  - SAP ID
  - Service ID
- **Group 5**
  - String
  - System ID

30 If one of the match criteria specified in step 6 is Encapsulation Tag Range, perform the following steps.

i Configure the Type parameter.

ii Configure the following parameters to define the outer encapsulation range:

- Outer Start Value (Tag1)
- Outer End Value (Tag1)

iii If you set the Type parameter to Q in Q, configure the following parameters to define the inner encapsulation range:

- Inner Start Value (Tag2)
- Inner End Value (Tag2)

31 Click on the Identification Strings tab.

32 Configure the Option Number parameter. The form displays additional parameters.

33 Configure the parameters.

- ANCP String
- Application Profile String
- Intermediate Destination ID
- SLA Profile String
- Subscriber Profile String
- Subscriber ID
- Category Map Name

34 Click on the Options tab.

35 To configure IPv4 options, perform the following steps.

i Click on the Create button. The Local User Database DHCP IPv4 Option form opens.

ii Configure the Option parameter. Depending on the Option value, different additional parameters must be configured.

iii If the Option parameter is set to Custom Option, Default Routers, DNS Name Servers, or Netbios Name Server, configure the following parameters:

- Number
- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

iv If the Option parameter is set to Lease Time, Lease Renew Time, or Lease Rebind Time, configure the following parameters:

- Days
- Hours
- Minutes
- Seconds

v If the Option parameter is set to Domain Name, configure the Value parameter.

vi If the Option parameter is set to Netbios Node Type, configure the Netbios Node Type parameter.

vii If the Option parameter is set to Subnet Mask, configure the IP Address 1 parameter.

viii Click on the OK button. A dialog box appears.

ix Click on the OK button. The Local User Database DHCP Option form closes and the Local User DB DHCP Host form lists the new options.

36 To configure IPv6 options, perform the following steps.

i Click on the IPv6 tab.

ii Click on the Create button. The Local User Database DHCP IPv6 Option form opens.

iii Configure the parameters:

- IPv6 Address 1
- IPv6 Address 2
- IPv6 Address 3
- IPv6 Address 4

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Local User Database DHCP Option6 form closes and the Local User DB DHCP Host form lists the new options.

37 Click on the OK button.

38 Click on the RADIUS Proxy Cache tab.

39 Configure the Routing Instance parameter.

40 If you set the Routing Instance parameter to Base, go to step 42.

41 Click on the Select button in the VPRN Service panel to choose a VPRN service from the Select VPRN Service form.

42 Click on the Select button in the RADIUS Proxy Server panel to choose a RADIUS proxy server from the Select RADIUS Proxy Server form.

43 Configure the Match Type parameter.

44 Perform one of the following:

a If the Match Type parameter is set to MAC Address, configure the MAC Address Format parameter.



Note — Select the Show Format check box to display the valid parameter options and the format that each option represents.

b If the Match Type parameter is set to Option, configure the Match Option parameter.

45 Configure the Match Failure Action parameter.

46 Click on the OK button. A dialog box appears.

47 Click on the OK button. The host specification is listed on the Local User Database form.

48 Click on the PPP tab. The PPP Match List form opens.

49 Configure the parameters.

- Match Type PPP 1
- Match Type PPP 2
- Match Type PPP 3



Note — You cannot set two parameters to the same value.

50 Click on the Masks tab.

51 Click on the Create button. The Local User Database PPP Mask form opens.

52 Configure the parameters.

- Match Type
- Prefix String
- Prefix Length
- Suffix String
- Suffix Length



Note — You must configure the Mask Type parameter before you configure the remaining parameters.

53 Click on the OK button. A dialog box appears.

54 Click on the OK button. The Local User Database PPP Mask form closes.

55 Click on the Hosts tab.

56 Click on the Create button. The Local User DB PPP Host form opens with the General tab displayed.

57 Configure the parameters.

- Host Name
- Administrative State
- Retail Service ID
- PADO Delay

58 Use the Select button in the Subscriber Pre-authentication Policy panel to choose a subscriber pre-authentication policy from the Select Subscriber Pre-authentication Policy form.

59 Use the Select button in the Subscriber Authentication panel to choose a subscriber authentication policy from the Select Subscriber Authentication Policy form.

60 Use the Select button beside the MSAP Policy Name parameter to choose an MSAP policy from the MSAP Policy form.

61 Use the Select button beside the MSAP Service ID parameter to choose an MSAP service ID from the Service form.

62 Perform one of the following.

a Use the Select button beside the MSAP Group Interface Name field to choose a group interface from the Group Interface form.

b Manually specify a group interface. Perform the following steps.

i Type the group interface name in the MSAP Group Interface Name field.

ii If the port ID is not included in the typed name, set one of the following parameters to Port ID, depending on whether the port ID is to be the prefix or suffix of the group interface name:

- MSAP Group Interface Prefix
- MSAP Group Interface Suffix



Note — If the combined length of the port ID and the typed name exceeds 32 characters, an alarm is raised.

63 Use the Select button beside the RADIUS Accounting Policy field to choose a RADIUS accounting policy from the Select RADIUS Accounting Policy form.

64 Use the Select button beside the Duplicate RADIUS Accounting Policy field to choose a duplicate RADIUS accounting policy from the Select RADIUS Accounting Policy form.

65 Configure the parameters on the Access Loop Information panel, if required:

- Circuit ID Type
- Circuit ID
- Remote ID Type
- Remote ID



Note — The Circuit ID parameter must be configured if the Circuit ID Type parameter is set to ASCII. The Remote ID parameter must be configured if the Remote ID Type parameter is set to ASCII.

66 Click on the Address tab.

67 Perform one of the following.

a Configure the following parameters:

- IP Address
- IP Address Prefix Length

b Select the Use Gateway Interface (GI) Address parameter.

68 Perform one of the following.

a Configure the following parameters:

- IP Address Pool Name
- Second IP Address Pool Name

b Configure the following parameters:

- Use Pool From Client
- Pool Name Delimiter

69 Configure the IPv6 addressing parameters, as required:

- IPv6 Address
- IPv6 Delegated Prefix (or IPv6 Prefix)
- Prefix Length
- IPv6 Delegated Prefix Length
- IPv6 Delegated Prefix Pool
- IPv6 WAN Address Pool
- IPv6 SLAAC Prefix
- Prefix Length

70 Click on the Host Identification tab.

71 Configure up to three of the following parameter groups.

- Circuit ID Format
- MAC Address
- Remote ID Format
- Service Name
- Circuit ID
- Remote ID
- SAP ID

72 Configure the following parameters:

- User Name Format
- User Name
- Password Type
- Password

73 If one of the match criteria specified in step 49 is Encapsulation Tag Range, perform the following steps.

i Configure the Type parameter.

ii Configure the following parameters to define the outer encapsulation range:

- Outer Start Value (Tag1)
- Outer End Value (Tag1)

iii If you set the Type parameter to Q in Q, configure the following parameters to define the inner encapsulation range:

- Inner Start Value (Tag2)
- Inner End Value (Tag2)

74 Click on the Identification Strings tab. Configure the Option Number parameter. The form displays additional parameters.

75 Configure the parameters, as required.

- ANCP String
- Application Profile
- Intermediate Destination ID
- SLA Profile String
- Subscriber Profile String
- Subscriber ID

76 Click on the L2TP tab.



Note — L2TP configuration is required on an NE that has the LAC role if RADIUS authentication is not used for PPP clients.

77 Use the Select button beside the Group Name parameter to choose a tunnel group from the Select Tunnel Group Name form.

78 Click on the Options tab.

79 To configure IPv4 options, perform the following steps.

i Click on the Create button. The Local User Database PPP Option form opens.

ii Configure the Option parameter. Depending on the Option value, different additional parameters must be configured.

iii If the Option parameter is set to DNS Name Servers, or Netbios Name Server, configure the following parameters:

- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

iv If the Option parameter is set to Custom Option, configure the following parameters:

- Number
- Type

v Depending on the setting of the Type parameter, configure any of the following parameters, as they appear:

- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4
- Value (for ASCII String or Hex String option types)

vi Click on the OK button. A dialog box appears.

vii Click on the OK button. The Local User Database DHCP Option form closes and the Local User DB DHCP Host form lists the new options.

80 To configure IPv6 options, perform the following steps.

i Click on the IPv6 tab.

ii Click on the Create button. The Local User Database PPP Option6 form opens.

iii Configure the parameters:

- IPv6 Address 1
- IPv6 Address 2
- IPv6 Address 3
- IPv6 Address 4

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Local User Database PPP Option6 form closes and the Local User DB DHCP Host form lists the new options.

81 Click on the Access Loop tab.

82 Click on the Create button. The Access Loop form opens.

83 Configure the parameters:

- Rate Down (kbps)
- Encap Offset Mode
- Encap Offset

84 Click on the OK button. A dialog box appears.

85 Click on the OK button. The Access Loop form closes.

86 Click on the OK button. The Local User DB PPP Host form closes.

87 Click on the OK button. A dialog box appears.

88 Click on the OK button.The Local User Database form closes.

89 Close the Manage Residential Subscribers form.

Procedure 65-6 To enable or disable subnet draining on a local DHCPv4 server

Perform this procedure to configure IP address draining for a subnet on a local DHCPv4 server. When subnet draining is enabled, the server stops leasing IP addresses from the subnet to new subscriber hosts; existing leases are not affected.

1 Perform one of the following.

   a Configure subnet draining on a base routing instance. Perform the following steps.

      i Choose Routing from the navigation tree view selector. The navigation tree displays the Routing view.

      ii Navigate to the required routing instance. The path is Network→NE→Routing Instance.

      iii Right-click on the routing instance and choose Properties. The Routing Instance (Edit) form opens with the General tab displayed.

   b Configure subnet draining on a VPRN routing instance. Perform the following steps.

      i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

      ii Configure the filter criteria, as required, and click on the Search button. A list of services is displayed.

      iii Select the required VPRN in the list and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

      iv Expand the Sites object in the navigation tree.

      v Select the required routing instance object. The Site (Edit) form opens with the General tab displayed.

2 Click on the Local DHCP Servers tab. The DHCPv4 tab lists the local DHCPv4 servers.

3 Select the required server in the list and click on the Properties button. The Local DHCP Server (Edit) form opens.

4 Click on the IP Address Pools tab. The IP address pools are listed.

5 Select the required pool and click on the Properties button. The IP Address Pool (Edit) form opens with the General tab displayed.

6 Click on the Subnets tab. The subnets are listed.

7 Select the required subnet and click on the Properties button. The Subnet (Edit) form opens with the General tab displayed.

8 Perform one of the following.

a Select the Subnet Drain parameter to enable draining of the subnet.

After the configuration change is applied, the DHCP server stops leasing IP addresses from the subnet.

b Deselect the Subnet Drain parameter to disable draining of the subnet.

After the configuration change is applied, the DHCP server leases IP addresses from the subnet.

9 Click on the OK button. The Subnet (Edit) form closes, and a dialog box appears.

10 Click on the OK button. The IP Address Pool (Edit) form reappears.

11 Click on the OK button. The IP Address Pool (Edit) form closes, and a dialog box appears.

12 Click on the OK button. The Local DHCP Server (Edit) form reappears.

13 Click on the OK button. The Local DHCP Server (Edit) form closes, and a dialog box appears.

14 Click on the OK button. The Routing Instance or Site (Edit) form reappears.

15 Click on the OK button. A dialog box appears.

16 Click on the Yes button. The Routing Instance or Site (Edit) form closes.

17 Close the Manage Services form, if required.

Procedure 65-7 To configure NE SHCV event handling

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Click on the View SHCV button. The Subscriber Host Connectivity Verification form opens.

3 Choose Network Element SHCV from the object drop-down list.

4 Configure the filter criteria and click on the Search button. A list of NEs appears.

5 Select an NE and click on the Properties button. The Network Element SHCV (Edit) form opens with the General tab displayed.

6 Configure the parameters:

- Trap Dropped Raises Alarm
- Rate Exceeded Raises Alarm
- Maximum Sessions Per MAC

7 Click on the OK button. The Network Element SHCV (Edit) form closes, and a dialog box appears.

8 Click on the Yes button.

9 Close the Subscriber Host Connectivity Verification form.

10 Close the Manage Residential Subscribers form.

Procedure 65-8 To retrieve PPPoA sessions

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Subscribers form opens.

2 Choose PPPoA Session (PPP Policy and Session) from the object drop-down list in the Manage Subscribers form.

3 Click on the Select button beside the Site ID parameter. The Select an ESM Capable Network Element form opens.

4 Select a network element from the list and click on the OK button. The Select an ESM Capable Network Element form closes.

5 Click on the Select button beside the Service ID parameter. The Select a Service Site form opens.

6 Select a service site from the list and click on the OK button. The Select a Service Site form closes.

7 Click on the Select button beside the Service Access Point parameter. The Select a Service Access Point form opens.

8 Select a service access point from the list and click on the OK button. The Select a Service Access Point form closes.

9 Click on the Search button. A list of applicable PPPoA sessions appears.

10 Select a PPPoA session from the list and click on the Properties button. The PPPoA Session form opens.

11 Review the PPPoA session information.

12 Close the PPPoA Session form.

13 Close the Manage Subscribers form.

Procedure 65-9 To configure a MEP on an SDP Binding

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a service and click on the Properties button. The service configuration form opens with the General tab displayed.

4 On the navigation tree, click on the site on which you want to configure a MEP on an SDP Binding; expand the entries for that site.



Note — MEPs can be configured on a SDP Binding for VPLS, VPRN, and VLL Epipe services.

5 Click on the Spoke SDP Bindings icon to display the site Spoke SDP Bindings.

6 Select one or more Spoke SDP Bindings, right-click, and choose Properties. The Spoke SDP Bindings configuration form opens with the General tab displayed.

7 Click on the Meps tab.

8 Click on the Create button. The MEP (Create) form opens.

9 Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

10 Select an entry and click on the OK button. The Select Maintenance Entity Group form closes.

11 Configure the parameters:

- Auto-Assign ID
- ID
- Site ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- Mac Address
- Fault Propagation
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)
- CCM Padding Packet Size (Bytes)



Note — The CCM Padding Packet Size (Bytes) parameter cannot be configured when the CCM interval parameter is set to 10 ms or 100 ms.

12 If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab. Otherwise, go to step 16.

13 Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

14 Click on the AIS tab.

15 Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

16 Click on the OK button. A dialog box appears.

17 Click on the OK button. The MEP (Create) form closes.

18 Close the Manage Services form.

Procedure 65-10 To configure L2Aware static port forwarding on a residential subscriber instance

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Residential Subscriber Instance from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of residential subscriber instances appears.

4 Select a residential subscriber instance and click on the Properties button. The Residential Subscriber Instance (Edit) form opens with the General tab displayed.

5 Click on the NAT Static Port Forwarding tab.

6 Click on the Create button. The NAT Static Port Forwarding Display (Create) form opens.

7 Configure the parameters:

- Inside IP Address
- Outside IP Address
- Inside Port
- Protocol
- Outside Port
- Lifetime (seconds)



Note — You cannot specify the same set of Inside Port and Protocol values in more than one static port mapping to an Inside IP Address.

You can specify the same Outside Port value in multiple mappings to an Inside IP Address.

8 Click on the OK button. The NAT Static Port Forwarding Port Display (Create) form closes, and the new entry is listed on the Residential Subscriber (Edit) form.

9 Perform the following steps to synchronize NAT static port forwards, if required.

i Choose one or more static port forwards from the list and click on the Sync button. The NAT Static Port Forwarding Sync form opens. You can choose up to 100 static port forwards.

ii Click on the Select button in the Targeted Router Instance panel. The Select Targeted Router Instance form opens.

iii Configure the Suppress Duplicate Error parameter.

iv Select a router instance from the list and click on the OK button. The Select Targeted Router Instance form closes and the NAT Static Port Forwarding Sync form reappears with the router instance information displayed.

v Configure the Lifetime (seconds) parameter and click on the OK button. A dialog box appears.

vi Click on the OK button.

10 Close the Residential Subscriber (Edit) form.

11 Close the Manage Residential Subscribers form.

Procedure 65-11 To resynchronize static port forwarding entries

Because of the potentially large number of static port forwarding entries, the entries are not resynchronized during a full NE resynchronization. Perform this procedure to manually resynchronize the entries, if required.



Note — The 5620 SAM static port forwarding entries are current and do not require resynchronization if the following conditions are true.

- The 5620 SAM is used to create, maintain, and delete each entry.
- Each entry has an infinite lifetime, so is truly static.

1 Right-click on an NE in the navigation tree and choose Resync→Customized Resync from the contextual menu. The Resync Sites step form opens with the Resync Options step displayed.

2 Select Choose MIB entries.

3 Click on the Next button. The Choose MIB Entries step is displayed.

4 Select tmnxNatFwdEntry in the list.

5 Click on the Next button. The Force Resync step is displayed.

6 Select the Ignore Timestamps parameter.

7 Click on the Finish button. The entries are refreshed.



Note — You can view the static port forwarding entries on the NAT Static Port Forwarding tab of the NAT Configuration form for the following:

- base or service routing instances
- residential subscriber instances

Procedure 65-12 To collect, view, and clear host tracking statistics and information

Use this procedure to perform one or more of the following:

- collect, view, and clear on-demand host tracking statistics and information for one of the following:
  - residential subscriber instance
  - VPLS L2 access interface
  - IES service access point
  - VPRN service access point
- clear statistics and host tracking information for one of the following:
  - a VPLS, VPRN, or IES service site
  - residential subscriber host

See the *5620 SAM Statistics Management Guide* for general information about configuring and collecting statistics.

1 To collect, view, and clear on-demand host tracking statistics and information for a residential subscriber instance.

i Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

ii Choose Residential Subscriber Instance (Residential Subscriber) from the object drop-down list.

iii Configure the filter criteria and click on the Search button. A list of residential subscriber instances appears.

iv Choose a residential subscriber instance and click on the Properties button. The Residential Subscriber Instance (Edit) form opens with the General tab displayed.

v Click on the Statistics tab.

vi Choose Host Tracking Stats (Residential Subscriber) from the object drop-down list.

vii Click on the Collect button to collect the statistics.

viii Select a statistics record and click on the Properties button to view the record. The statistics record form opens.

ix View the statistics information.

x Click on the Close button to close the statistics record form.

xi Repeat steps viii to x for each statistics record that you want to view.

xii Click on the Host Tracking Info tab.

xiii Configure the filter criteria and click on the Search button. Host tracking data for the residential subscriber instance appears.

xiv Click on the Clear button. A dialog box appears.

xv If you only need to clear the host tracking statistics, enable the Clear only Host Tracking Statistics? check box.

xvi Click the Yes button. An information box appears.

xvii Click the OK button. The data is deleted from the NE.

xviii Click the Clear Status tab to view a list of host tracking information clear results.

xix Choose a request and click on the Properties button to view information about the request, if required.

xx Close the Residential Subscriber Instance (Edit) form.

xxi Close the Manage Residential Subscribers form.

2 To collect, view, and clear on-demand host tracking statistics and information for a VPLS L2 access interface.

i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

ii Choose VPLS Service (VPLS) from the object drop-down list.

iii Configure the filter criteria and click on the Search button. A list of VPLS services appears.

iv Select a service and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

v On the navigation tree, click on an access interface. The VPLS L2 Access Interface (Edit) form opens.

vi Click on the Statistics tab.

vii Choose Host Tracking Stats on SAP (Residential Subscriber) from the object drop-down list.

viii Click on the Collect button to collect the statistics.

ix Select a statistics record and click on the Properties button to view the record. The statistics record form opens.

x View the statistics information.

xi Click on the Close button to close the statistics record form.

xii Repeat steps ix to xi for each statistics record that you want to view.

xiii Click on the Subscriber Management tab.

xiv Click on the Host Tracking Info tab.

xv Configure the filter criteria and click on the Search button. Host tracking data for the L2 access interface appears.

xvi Click on the Clear button. A dialog box appears.

xvii If you only need to clear the host tracking statistics, enable the Clear only Host Tracking Statistics? check box.

xviii Click the Yes button. An information box appears.

xix Click the OK button. The data is deleted from the NE.

xx Repeat steps xvi to xix for each host that you need to clear.

xxi Click the Clear Status tab to view a list of host tracking information clear results.

xxii Choose a request and click on the Properties button to view information about the request, if required.

xxiii Close the VPLS L2 Access Interface (Edit) form.

xxiv Close the VPLS Service (Edit) form.

xxv Close the Manage Services form.

3 To collect, view, and clear on-demand host tracking statistics and information for an IES service access point.

i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

ii Choose IES Service (IES) from the object drop-down list.

iii Configure the filter criteria and click on the Search button. A list of IES services appears.

iv Select a service and click on the Properties button. The IES Service (Edit) form opens with the General tab displayed.

v On the navigation tree, click on a service access point. The IES Service Access Point (Edit) form opens.

vi Click on the Statistics tab.

vii Choose Host Tracking Stats on SAP (Residential Subscriber) from the object drop-down list.

viii Click on the Collect button to collect the host tracking statistics.

ix Select a statistics record and click on the Properties button to view the record. The statistics record form opens.

x View the statistics information.

xi Click on the Close button to close the statistics record form.

xii Repeat steps ix to xi for each statistics record that you want to view.

xiii Click on the Subscriber Management tab.

xiv Click on the Host Tracking Info tab.

xv Configure the filter criteria and click on the Search button. Host tracking data for the IES service access point appears.

xvi Click on the Clear button. A dialog box appears.

xvii If you only need to clear the host tracking statistics, enable the Clear only Host Tracking Statistics? check box.

xviii Click the Yes button. An information box appears.

xix Click the OK button. The data is deleted from the NE.

xx Repeat steps xvi to xix for each host that you need to clear.

xxi Click the Clear Status tab to view a list of host tracking information clear results.

xxii Choose a request and click on the Properties button to view information about the request, if required.

xxiii Close the IES Service Access Point (Edit) form.

xxiv Close the IES Service (Edit) form.

xxv Close the Manage Services form.

4 To collect, view, and clear on-demand host tracking statistics and information for a VPRN service access point.

i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

ii Choose VPRN Service (VPRN) from the object drop-down list.

iii Configure the filter criteria and click on the Search button. A list of VPRN services appears.

iv Select a service and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

v On the navigation tree, click on a service access point. The VPRN Service Access Point (Edit) form opens.

vi Click on the Statistics tab.

vii Choose Host Tracking Stats on SAP (Residential Subscriber) from the object drop-down list.

viii Click on the Collect button to collect the host tracking statistics.

ix Select a statistics record and click on the Properties button to view the record. The statistics record form opens.

x View the statistics information.

xi Click on the Close button to close the statistics record form.

xii Repeat steps vi to xi for each statistics record that you want to view.

xiii Click on the Subscriber Management tab.

xiv Click on the Host Tracking Info tab.

xv Configure the filter criteria and click on the Search button. Host tracking data for the VPRN service access point appears.

xvi Click on the Clear button. A dialog box appears.

xvii If you only need to clear the host tracking statistics, enable the Clear only Host Tracking Statistics? check box.

xviii Click the Yes button. An information box appears.

xix Click the OK button. The data is deleted from the NE.

xx Repeat steps xvi to xix for each host that you need to clear.

xxi Click the Clear Status tab to view a list of host tracking information clear results.

xxii Choose a request and click on the Properties button to view information about the request, if required.

xxiii Close the VPRN Service Access Point (Edit) form.

xxiv Close the VPRN Service (Edit) form.

xxv Close the Manage Services form.

5 To clear on-demand host tracking statistics and information for a VPLS service site.

i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

ii Choose VPLS Service (VPLS) from the object drop-down list.

iii Configure the filter criteria and click on the Search button. A list of VPLS services appears.

iv Select a service and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

v On the navigation tree, click on a site. The VPLS Site (Edit) form opens with the General tab displayed.

vi Click on the IGMP Host Tracking tab.

vii Click on the Clear button. A dialog box appears.

viii If you only need to clear the host tracking statistics, enable the Clear only Host Tracking Statistics? check box.

ix Click the Yes button. An information box appears.

x Click the OK button. The service site data is deleted from the NE.

xi Click the Clear Status tab to view a list of site host tracking information clear results.

xii Choose a request and click on the Properties button to view information about the request, if required.

xiii Close the VPLS Site (Edit) form.

xiv Close the VPLS Service (Edit) form.

xv Close the Manage Services form.

6 To clear on-demand host tracking statistics and information for an IES service site.

i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

ii Choose IES Service (IES) from the object drop-down list.

iii Configure the filter criteria and click on the Search button. A list of IES services appears.

iv Select a service and click on the Properties button. The IES Service (Edit) form opens with the General tab displayed.

v On the navigation tree, click on a site. The IES Site (Edit) form opens with the General tab displayed.

vi Click on the IGMP Host Tracking tab.

vii Click on the Clear button. A dialog box appears.

viii If you only need to clear the host tracking statistics, enable the Clear only Host Tracking Statistics? check box.

ix Click the Yes button. An information box appears.

x Click the OK button. The service site data is deleted from the NE.

xi Click the Clear Status tab to view a list of site host tracking information clear results.

xii Choose a request and click on the Properties button to view information about the request, if required.

xiii Close the IES Site (Edit) form.

xiv Close the IES Service (Edit) form.

xv Close the Manage Services form.

7 To clear on-demand host tracking statistics and information for a VPRN service site.

i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

ii Choose VPRN Service (VPRN) from the object drop-down list.

iii Configure the filter criteria and click on the Search button. A list of VPRN services appears.

iv Select a service and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

v On the navigation tree, click on a site. The VPRN Site (Edit) form opens with the General tab displayed.

vi Click on the IGMP Host Tracking tab.

vii Click on the Clear button. A dialog box appears.

viii If you only need to clear the host tracking statistics, enable the Clear only Host Tracking Statistics? check box.

ix Click the Yes button. An information box appears.

x Click the OK button. The service site data is deleted from the NE.

xi Click the Clear Status tab to view a list of site host tracking information clear results.

xii Choose a request and click on the Properties button to view information about the request, if required.

xiii Close the VPRN Site (Edit) form.

xiv Close the VPRN Service (Edit) form.

xv Close the Manage Services form.

8 To clear on-demand host tracking statistics and information for a residential subscriber host.

i Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

ii Choose Residential Subscriber Host (Residential Subscriber) from the object drop-down list.

iii Select the Search Current Subscriber Host Information option.

iv Click on the Select buttons to specify the site, service ID, and service access point for which you want to view subscriber host information.

v Configure the Inner Encapsulation Value and Outer Encapsulation Value parameters.

The Outer Encapsulation Value parameter is configurable only when the port encapsulation type is Dot1 Q or Q in Q. The Inner Encapsulation Value parameter is configurable only when the port encapsulation type is Q in Q.

vi Click the Search button. A list of hosts appears.

vii Choose a host from the list and click the Clear Host Tracking button. A dialog box appears.

viii If you only need to clear the host tracking statistics, enable the Clear only Host Tracking Statistics? check box.

ix Click the Yes button. An information box appears.

x Click the OK button. The residential subscriber host data is deleted from the NE.

xi You can view a list of the residential host clear results by clicking on the Clear Status button on the residential subscriber instance form.

xii Repeat steps vii to xi for each host that you need to clear.

xiii Close the Manage Residential Subscribers form.

Procedure 65-13 To view subscriber host information

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Residential Subscriber Host from the object list.

3 Click on the Select buttons to specify the site, service ID, and service access point for which you want to view subscriber host information.

4 Configure the Inner Encapsulation Value and Outer Encapsulation Value parameters.

The Outer Encapsulation Value parameter is configurable only when the port encapsulation type is Dot1 Q or Q in Q. The Inner Encapsulation Value parameter is configurable only when the port encapsulation type is Q in Q.

5 Click on the Search button. A list of subscriber hosts is returned.

6 Select a subscriber host in the list and click on the Properties button. The Subscriber Host form appears.

7 View the available read-only attributes.

8 To retrieve subscriber service information for the subscriber host, perform the following steps:

i Click on the Subscriber Services tab.

ii Click on the Search button. A list of subscriber service items is returned.

iii Select an item in the list and click on the Properties button. The Subscriber Service form appears.

iv View the available read-only attributes.

v Click on the Cancel button to close the Subscriber Service form.

9 Click on the Cancel button to close the Subscriber Host form.

Procedure 65-14 To view a subscriber and the associated subscriber hosts



Note — You can use the 5620 SAM GUI to display the object model associated with 5750 SSC residential subscriber services.

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Residential Subscriber from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of residential subscribers appears.

4 Select a residential subscriber and click on the Properties button. The Residential Subscriber (View) form opens with the General tab displayed.

5 View a list of the residential subscriber instances for the subscriber, if required.

i Click on the Residential Subscriber Instances tab.

ii Select a residential subscriber instance and click on the Properties button. The Residential Subscriber Instance (Edit) form opens with the General tab displayed.

iii View the instance information.

The Residential Subscriber State panel displays the following subscriber status information:

- Active
- Residential Subscriber Creation
- Last Active State Change

iv Close the Residential Subscriber Instance (Edit) form.

6 Specify the subscribed application profile for AA reporting, if required.

i Click on the Residential Subscriber Instances tab.

ii Select a residential subscriber instance and click on the Properties button. The Residential Subscriber Instance (Edit) form opens with the General tab displayed.

iii Configure the Subscribed Application Profile parameter.

iv Click on the OK button. A dialog box appears.

v Click on the Yes button.

7 List and view the active hosts for the subscriber, if required.

i Click on the Subscriber Hosts tab.

ii Click on the Find button. A confirmation prompt appears.

iii Click on the Yes button. The list of subscriber hosts refreshes with the active subscriber host entries.

iv To view the information for a subscriber host, select the host and click on the Properties button. The Subscriber Host form opens with the subscriber host information displayed. Otherwise, go to step 8.

v View the subscriber host information.

vi Close the Subscriber Host form.

8 Close the Residential Subscriber (View) form.

9 Close the Manage Residential Subscribers form.

Procedure 65-15 To view a subscriber instance and its related information



Note — You can use the 5620 SAM GUI to display the object model associated with 5750 SSC residential subscriber services.

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Residential Subscriber Instance from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of residential subscriber instances appears.

4 Select a residential subscriber instance and click on the Properties button. The Residential Subscriber Instance (Edit) form opens with the General tab displayed.

The Residential Subscriber State panel displays the following subscriber status information:

- Active
- Residential Subscriber Creation
- Last Active State Change

5 View ANCP subscriber line information for the subscriber instance, if required.

i Click on the ANCP Subscriber Line Rates tab.

ii View the line rate information.

iii To query DSL line information for the residential subscriber instance, click on the Search button. (You are prompted to confirm the query action.)

The DSL line information is listed at the bottom of the form.

6 List and view the active hosts for the subscriber instance, if required.

i Click on the Subscriber Hosts tab.

ii Click on the Find button. A confirmation prompt appears.

iii Click on the Yes button. The list of subscriber hosts refreshes with the active subscriber host entries.

iv To view the information for a subscriber host, select the host and click on the Properties button. The Subscriber Host form opens with the subscriber host information displayed. Otherwise, go to step 9.

v View the subscriber host information.

vi Click on the Cancel button to close the Subscriber Host form.

7 List and view the subscriber hosts for which a DHCP lease has been manually terminated, if required.

i Click on the Clear Status tab.

ii To view the information for a subscriber host, select the host and click on the Properties button. The Subscriber Host form opens with the subscriber host information displayed. Otherwise, go to step 9.

iii View the subscriber host DHCP lease information.

iv Click on the Cancel button to close the Subscriber Host form.

8 List and view IGMP hosts for the subscriber instance, if required. Otherwise, go to step 9.

i Click on the IGMP Hosts tab.

ii Click on the Search button. A confirmation prompt appears.

iii Click on the Yes button. The list of IGMP hosts refreshes with the active IGMP host entries.

iv To view the information for an IGMP host, select the host and click on the Properties button. The IGMP Host form opens with the General tab displayed.

v View the IGMP host information on the General tab.

vi Click on the Groups tab to view IGMP host groups associated with the IGMP host.

vii To view the information for an IGMP host group, select the group and click on the Properties button. The IGMP Host Group form opens with the General tab displayed.

viii View the IGMP host group information on the General tab.

ix Click on the Sources tab to view IGMP host group sources associated with the IGMP host.

x To view the information for an IGMP host group source, select the source and click on the Properties button. The IGMP Host Group Source form opens with the General tab displayed.

xi View the IGMP host group source information on the General tab.

xii Click on the Cancel button to close the IGMP Host Group Source form.

xiii Click on the Cancel button to close the IGMP Host Group form.

xiv Click on the Cancel button to close the IGMP Host form.

9 View the collected statistics for the subscriber instance, if required.

i Click on the Statistics tab.

ii Choose a statistics class from the object drop-down list.

iii Click on the Collect button to collect the statistics for the chosen class, or click on the Collect All button to collect the statistics for all classes.

iv Select a statistics record and click on the Properties button to view the record. The statistics record form opens.

v View the statistics information.

vi Click on the Close button to close the statistics record form.

vii Repeat steps ii to vi for each statistics class that you want to view.

10 Click on the Cancel button to close the Residential Subscriber Instance (Edit) form.

11 Close the Manage Residential Subscribers form.

Procedure 65-16 To view DHCP lease information

Use this procedure to retrieve DHCP lease information from a subscriber host in the network. The DHCP information available to the 5620 SAM varies depending on the network elements used by the subscriber.

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose DHCP Lease State from the object drop-down list.

3 Click on the Search button beside the Site ID parameter and select the site of the subscriber host.

4 Click on the Search button beside the Service parameter and select a service from the site you selected in step 3.

5 Configure the filter criteria and click on the Search button. A list of DHCP leases appears.

6 Select a DHCP lease from the list and click on the Properties button. The DHCP Lease State form opens.

7 View the DHCP lease information.

8 Close the DHCP Lease State form.

9 Close the Manage Residential Subscribers form.

Procedure 65-17 To view SLA policy instances on a subscriber instance

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Residential Subscriber Instance from the Object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of residential subscriber interfaces appears.

4 Select a residential subscriber interface and click on the Properties button. The Residential Subscriber Interface form opens.

5 Click on the SLA Instances tab.

6 Configure the filter criteria and click on the Search button. A list of SLA profile instances appears.

7 Select an SLA instance and click on the Properties button. The SLA Profile Instance form appears.

8 View the SLA profile instance information.

9 Close the SLA Profile Instance, Residential Subscriber Interface, and Manage Residential Subscribers forms.

Procedure 65-18 To view SHCV log events

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Click on the View SHCV button. The Subscriber Host Connectivity Verification form opens.

3 Choose SHCV Event Log from the object drop-down list.

4 Configure the filter criteria and click on the Search button. A list of NE SHCV event logs appears.

5 Select a log entry and click on the Properties button. The SHCV Log Entry form opens.

6 View the log entry.

7 Close the SHCV Log Entry form.

8 Close the Subscriber Host Connectivity Verification form.

9 Close the Manage Residential Subscribers form.

Procedure 65-19 To change the identification of a subscriber

Perform this procedure to change the identification of a subscriber, for example, when you no longer want hosts on the SAP to use the SAP ID as the subscriber ID.



Caution 1 — Renaming a subscriber can be service-affecting because it changes the subscriber identification string of all associated subscriber hosts. Before you proceed, ensure that no subscriber hosts require the subscriber identification string associated with this subscriber.

Caution 2 — Renaming a subscriber changes the SAP default subscriber identification strings that are associated with it.

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Residential Subscriber from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of residential subscribers appears.

4 Select a residential subscriber and click on the Modify button. The Residential Subscriber (Edit) form opens with the General tab displayed.

5 Configure the New Subscriber Identification parameter.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The 5620 SAM renames the subscriber.

8 Close the Manage Residential Subscribers form.

Procedure 65-20 To reset a subscriber's subscription credit limit

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form appears.

2 Choose Residential Subscriber Host from the Object Type drop-down list.

3 Click on the Select buttons to specify the site, service ID, and service access point for which you want to view subscriber host information.

4 Configure the Inner Encapsulation Value and Outer Encapsulation Value parameters.

The Outer Encapsulation Value parameter is configurable only when the port encapsulation type is Dot1 Q or Q in Q. The Inner Encapsulation Value parameter is configurable only when the port encapsulation type is Q in Q.

5 Click on the Search button. A list of residential subscriber hosts is displayed.

6 Perform one of the following:

a Select a host from the list and click on the Reset Credit button. Go to step 11.

b Select a host from the list and click on the Properties button. The Subscriber Host form opens.

7 Click on the Credit Control Operational values tab.

8 Select an entry from the list and perform one of the following:

a Click on the Reset Credit button. Go to step 10.

b Click on the Properties button. A form opens.

9 Close the form after viewing credit control data.

10 Close the Subscriber Host form.

11 Close the Manage Residential Subscribers form.

Procedure 65-21 To modify the primary subscriber identification script or URL

This procedure allows a 5620 SAM operator to modify the primary subscriber identification script without service disruption. Perform this procedure only when the primary script and URL are operational.



Caution — Modifying the primary subscriber identification script is potentially service-affecting if no functional backup script is administratively enabled. Modifying a backup (secondary or tertiary) subscriber identification script is unlikely to be service-affecting if the other backup script (secondary or tertiary) functions properly and is administratively enabled. Ensure that at least one administratively enabled backup script is accessible to the 5620 SAM and the NEs to which it applies before you proceed.

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Choose Subscriber Identification Policy from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of subscriber identification policies appears.

4 Select a subscriber identification policy and click on the Properties button. The Subscriber Identification Policy (Edit) form opens with the General tab displayed.

5 Copy the operational primary script URL to the secondary position. This action ensures that an operational backup script is in place in the event that there is a problem with the new primary script or URL.

   i Set the Secondary Script Administrative State parameter to disabled.

   ii Click on the Apply button. A dialog box appears.

   iii Click on the Yes button. The 5620 SAM administratively disables the secondary script.

   iv Configure the Secondary Script URL parameter with the value of the Primary Script URL parameter.

   v Set the Secondary Script Administrative State parameter to enabled.

   vi Click on the Apply button. A dialog box appears.

   vii Click on the Yes button. The 5620 SAM administratively enables the secondary script.



Note — You must administratively disable and enable a script URL to cause the NEs to which the subscriber identification policy applies to load the script using the URL.

6 Modify a renamed copy of the former primary script or create a replacement script, as required; record the new or modified script URL.

7 Configure the new URL as the primary script URL.

i Set the Primary Script Administrative State parameter to Disabled.

ii Click on the Apply button. A dialog box appears.

iii Click on the Yes button. The 5620 SAM administratively disables the primary script. The secondary (former primary) script is the active script.

iv Configure the Primary Script URL parameter with the new URL value.

v Set the Primary Script Administrative State parameter to Enabled.

vi Click on the Apply button. A dialog box appears.

vii Click on the Yes button. The 5620 SAM administratively enables the primary script. The new primary script is the active script.



Note — You must administratively disable and enable a script URL to cause the NEs to which the subscriber identification policy applies to load the script using the URL.

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button. The Subscriber Identification Policy (Edit) form closes.

10 Close the Manage Subscriber Policies form.

Procedure 65-22 To delete an inactive residential subscriber instance

Use this procedure to remove the record of an inactive residential subscriber instance from the 5620 SAM database. Residential subscriber instances become inactive in the 5620 SAM when the subscriber is deleted from the NE.



Note — AA statistics data can be lost when you delete a residential subscriber instance before the 5620 SAM is finished collecting and processing AA statistics. Alcatel-Lucent recommends waiting at least two statistics collection intervals before deleting an inactive residential subscriber instance.

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Residential Subscriber Instance from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of residential subscriber instances appears.

The Active property indicates the status of each residential subscriber instance in the list. An inactive residential subscriber instance has no check mark under the Active heading.

4 Select the inactive residential subscriber instance you want to delete and click on the Delete button. The inactive residential subscriber instance is removed from the list.

5 Close the Manage Residential Subscribers form.

65.6 SAP and MSAP management

You can use residential subscriber profiles and policies to manage SAPs. Enabling residential subscriber management on a SAP does not affect an existing dynamic host on a SAP until the host DHCP lease expires, at which point a subscriber identification policy manages lease renewal. Static hosts require the provisioning of a subscriber identification string for continued network access.

When residential subscriber management on a SAP is enabled, each subscriber host that connects to the SAP requires a subscriber identification string to associate the host with a subscriber instance on the NE, or network access is denied. A subscriber identification string uniquely identifies a subscriber in the 5620 SAM.

The maximum number of subscribers that can use a SAP is configurable. When a SAP is limited to one subscriber, you can specify the treatment of traffic that does not match the subscriber profile, such as BTV traffic, which uses an IP address in the multicast range as the destination address. During single-subscriber SAP configuration, the 5620 SAM operator specifies whether to allow non-profile traffic and specifies the SLA and subscriber profiles to use for non-profile traffic, if it is allowed.

SAP DHCP monitoring

You can monitor the DHCP events on one or more SAPs. A SAP monitoring form is available from the Manage Residential Subscribers form. Table 65-3 describes the DHCP monitoring events supported by the 5620 SAM.

Table 65-3 SAP DHCP monitoring events

DHCP event	Description
DHCP Lease Entries Exceeded	The number of DHCP lease state entries on a SAP has reached the configured maximum.
DHCP Lease State Overridden	An existing DHCP lease state was overridden by a new lease state with the same IP address and a new MAC address.
Suspicious DHCP Packet	A DHCP packet containing suspicious content was received.
DHCP ACK Dropped	A DHCP ACK message was discarded because the related lease state could not be updated.
Host Connectivity Lost	The connection to the specified host was lost.
Host Connectivity Restored	The connection to the specified host was regained.

The maximum number of SAPs that can be selected for monitoring is configurable through XML; the default is five. SAP monitoring has a performance impact, so only a small number are typically monitored at one time.

The Monitored Access Interface form displays a variety of DHCP-related events or notifications about subscriber hosts on a SAP that are compiled using traps received from NEs. You can also open an event log for the SAP from the SAP Properties form. The logged events include information on DHCP lease entries, lease states, and host connectivity. An entry is added to the table whenever a new event occurs. You can purge event entries using the Monitoring Configuration form.

SAP monitoring can be started, stopped, or removed from the monitoring configuration form, and the monitoring period can be configured.

The SAP monitored objects and the associated events are stored in the database. The monitoring continues until the monitoring period elapses or the monitoring is stopped by a 5620 SAM operator.

Managed SAP (MSAP)

You can configure the 5620 SAM to automatically create a SAP for a subscriber; this SAP is called a managed SAP, or MSAP. MSAPs are used in network models where each subscriber has a separate VLAN, and multiple subscriber hosts share a SAP. MSAP creation uses the authentication mechanisms that an NE supports to provide an MSAP for the one-subscriber-per-SAP model. An MSAP behaves the same as a regular SAP, but the MSAP configuration is not editable. MSAPs count towards the maximum number of SAPs allowed on an NE.

An MSAP is typically used by only one subscriber, although the 5620 SAM supports MSAPs shared by multiple subscribers. However, if more than one subscriber is allowed and an MSAP has been defined by a host, when a new host installation attempts to change the MSAP policy the installation fails and raises an event.

The creation of an MSAP is triggered by a capture SAP. When a capture SAP is configured, triggering packets initiate RADIUS authentication, and the RADIUS reply provides a service context. The authentication and the service context are used by the NE to create an MSAP. See "Creating a capture SAP" in this section for information about creating a capture SAP.

Although MSAPs are not configurable, a user with a Policy Management or Subscriber Management role can create, list, delete, or modify an MSAP policy to control how the parameters apply during MSAP creation.

An MSAP remains active as long as there is at least one subscriber host on the MSAP. See "MSAP management" in this section for more information about managing an MSAP.

MSAPs are supported in HA and dual-homing environments. In dual homing, the MSAP is synchronized with the other NE during MSAP creation. For both HA and dual-homing environments, each participating NE must use the same MSAP policy.

Creating a capture SAP

A capture SAP must be defined to trigger the process that automatically creates an MSAP. A capture SAP does not forward traffic. See Procedure 65-28 to configure a capture SAP.

You can create a capture SAP only in a VPLS. A capture SAP can create MSAPs in the routed CO configuration of an IES or VPRN, and in a VPLS TPSDA configuration. IES and VPRN MSAPs are restricted to group interfaces.

The following triggers are supported to initiate MSAP creation:

- DHCP Trigger Packets—DHCP Discover (or Requests if configured) for DHCP clients; the MSAP lifetime is defined by the lease time.
- PPPoE Trigger Packets—PPPoE PADI for PPPoE client; the MSAP lifetime is defined by the session time. The MSAP is installed after an IP address is provided.
- ARP Trigger Packets—ARP for static-ip hosts; the MSAP lifetime is defined by ARP entry time. Current ARP entry refresh behavior is maintained.

After you configure the capture SAP, every DHCP packet, PPPoE packet, or ARP packet received on the SAP is sent to the CPM, which triggers RADIUS authentication to provide a service context. The MSAP is created in the specified service. Non-triggering packets captured by the capture SAP are dropped.

If RADIUS does not provide all of the required information to install the host (for example, RADIUS lacks the IP address), the MSAP is created with a short timer while waiting for the host to be installed. Default SAP polices are available on the NE and will be used if the MSAP policy is not configured.

The authentication policy used in the capture SAP must be the same as the policy used for the MSAP. For L3, the authentication policy is defined under the group-interface.



Note 1 — When PPPoE is used with MSAPs, the authentication policy must not use the username for MSAP creation.

Note 2 — The MSAP is not created (and an event is generated) if the group-interface name returned from RADIUS points to a different authentication policy than the policy defined by the capture SAP.

For MSAPs, the authentication policy is defined in the MSAP policy. Based on the configuration, the system reauthenticates the sessions when they are renewed. If the authentication policy is not used or when only PPPoE is used, the MSAPs stay active when the session is renewed.

An MSAP is created with dual-pass (shared) queuing. The SLA profile of the host may change the queuing later in the process. An MSAP is always created with the default QoS and scheduling.

MSAP management

An MSAP cannot be modified directly, so MSAP management is performed using MSAP policies. To make changes to an MSAP, alter the MSAP policy for the MSAP and then re-evaluate the MSAP. During re-evaluation, the NE updates the MSAP based on the changes to the MSAP policy. See Procedure 65-31 for information about changing and re-evaluating an MSAP policy.



Warning — If there is a disruption on the NE and the NE recovers by restarting, all MSAPs are re-evaluated and any policy changes are applied.

The 5620 SAM treats the setup and teardown of MSAPs as state transitions to offset the load imposed by constant SAP creation and deletion. There are two states that an MSAP can have, active or inactive. These states cannot be configured. The state is automatically set to active when the MSAP is created on the NE. When the NE deletes the MSAP, the state changes to inactive, and the MSAP continues to be available in the 5620 SAM but is not used until it is reactivated by the NE. When the MSAP is reactivated, it will have the same identification so that the 5620 SAM can identify it with the same FDN.

The state information is not automatically updated in the 5620 SAM GUI. You must perform a resynchronization to retrieve the current state information. When the state is inactive, performance statistics for the MSAP are not retrievable; however, historical statistical records are available. You can schedule MSAP statistics or collect the statistics on demand. See the *5620 SAM Statistics Management Guide* for more information about scheduling and collecting statistics.

Inactive services that previously contained MSAPs consume database space. MSAPs that have been in an inactive state for a long period of time or that are no longer used must be manually deleted. See Procedure 65-34 for more information about deleting an MSAP.



Caution — The creation of a SAP that uses the same port and encapsulation values as an existing inactive MSAP fails under the following conditions:

- If you try to use the 5620 SAM to create a SAP, the configuration fails and the 5620 SAM displays an error message.
- If you use a CLI to create a SAP in a service other than the service that contains the MSAP, the configuration succeeds but the MSAP remains inactive until the regular SAP is deleted. Although the 5620 SAM displays the SAP and MSAP, the MSAP remains inactive and consumes resources.
- If you use a CLI to create a SAP in the service that contains the MSAP, the SAP creation fails.

Alcatel-Lucent recommends that you delete an inactive MSAP from the 5620 SAM if you need to create a regular SAP on the same port using the same encapsulation values. See Procedure 65-34 for more information about deleting MSAPs.

MSAP Re-evaluate Lease States function

The 5620 SAM Re-evaluate Lease States function allows you to push SLA profile or subscriber profile changes out to residential subscribers without reinstantiating the hosts. See Procedure 65-33 for information.

MSAP alarm suppression

An IES or VPRN MSAP that is created on a LAG in an SRRP deployment uses a 5620 SAM mechanism to suppress unnecessary AccessInterfaceDown alarms. The mechanism uses the SRRP states of the redundant BNGs, and determines whether to raise the alarm based on the following rules:

- When the active BNG is in the master SRRP state and the standby BNG is in the initialize or backupShunt SRRP state, no AccessInterfaceDown alarm is raised against the standby BNG.
- If the standby BNG reboots, or if there is a link failure between the standby BNG and the access network, the MSAP AccessInterfaceDown alarms are suppressed for the standby BNG. The active BNG continues to remain in the master SRRP state. In this scenario, there may be other alarms on the standby BNG for card or link failures.
- After a fault that results in an SRRP failover, for example, active BNG reboot or loss of access network connectivity on the active BNG, an AccessInterfaceDown alarm is raised against each BNG. The alarms clear after SRRP state convergence.
- After a fault that affects both BNGs concurrently and disables SRRP redundancy, an AccessInterfaceDown alarm is raised against each BNG. The alarms clear when a BNG regains connectivity and assumes the role of SRRP master.



Note — The alarm-suppression mechanism can function correctly only when SRRP is correctly configured. If an SRRP peer is missing or disabled, the alarms may not be suppressed for the BNG that the 5620 SAM perceives to be the standby BNG.

MSAP event logs

An MSAP event log records the date, time, and active state for each state change that occurs after the MSAP is created. An event log is not recorded when the MSAP is created, although the information is recorded in a time stamp. See Procedure 65-30 to view the event log for each MSAP, purge the event log records, and modify the global MSAP log policy retention time and administrative state.

MSAP time stamps

You can view the following MSAP state time stamps:

- date and time that the MSAP was created
- date and time of the last active state change

See Procedure 65-29 for information about viewing MSAP properties.

65.7 Workflow to manage MSAPs

1. Create an MSAP policy; see Procedure 54-5.
2. Create a capture SAP that references the MSAP policy you created in Step 1; see Procedure 65-28.

3 Change an existing MSAP by modifying and re-evaluating an MSAP policy, as required. To modify a single MSAP, see Procedure 65-31; to modify multiple MSAPs that use the same policy, see Procedure 65-32.

4 Perform the following MSAP maintenance tasks, as required:

a List MSAPs; see Procedure 65-29.

b View or purge MSAP logs, or modify the MSAP log policy; see Procedure 65-30.

c Delete an MSAP; see Procedure 65-34.

d Delete an MSAP policy; see Procedure 65-35.

65.8 SAP managment procedures

Use the following procedures to perform SAP management tasks.

Procedure 65-23 To manage residential subscriber management components on a SAP

Perform this procedure to manage the subscriber configuration on one or more SAPs. You can configure the subscriber-related SAP parameters and assign one or more of the following residential subscriber management components:

- subscriber identification policy
- default subscriber identification string
- default subscriber profile
- default SLA profile
- non-subscriber traffic subscriber profile
- non-subscriber traffic SLA profile

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a service and click on the Properties button. The service configuration form opens with the General tab displayed.

4 On the navigation tree, click on the site on which you want to manage the SAPs; expand the entries for that site.

5 Click on the Access Interfaces icon to display the site SAPs.

6 Select one or more SAPs, right-click, and choose Properties. The SAP configuration form opens with the General tab displayed.



Note 1 — You can configure subscriber management on multiple SAPs at once from any list of SAP search results that the 5620 SAM generates. For simplicity, the procedure uses the term SAP to mean one or more SAPs, and focuses only on SAPs that belong to the same service site.

Note 2 — The 5620 SAM commits changes to a SAP configuration only when subscriber management is enabled on all SAPs that you are configuring.

7 Click on the Subscriber Management tab. The Host Connectivity tab is displayed.

8 Click on the Profiles tab.

9 Perform one of the following steps for a component.

a Associate a component with the SAP.

i Click on the Select button beside the component in the Policies panel. The component Select Default form opens.

ii Select a component and click on the OK button. The component Select Default form closes, and the Policies panel refreshes with the component name.

b Remove a component, or replace an existing component with a new component.



Caution — Removing or replacing a residential subscriber management component on a SAP that is in use by subscriber hosts can be service-affecting to hosts that attempt to join the network. Ensure that removing the component does not affect the subscriber hosts before you proceed.

i Click on the Clear button beside the component in the Policies panel. The 5620 SAM removes the component from the Policies panel.

ii If you want to choose a component to replace the removed component, go to step 9 a.

10 Click on the OK button. The SAP configuration form closes.

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The service configuration form closes.

13 Close the Manage Services form.

Procedure 65-24 To enable or disable residential subscriber management on a SAP

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a service and click on the Properties button. The service configuration form opens with the General tab displayed.

4 On the navigation tree, click on the site on which you want to enable or disable residential subscriber management on a SAP; expand the entries for that site.

5 Click on the Access Interfaces icon to display the site SAPs.

6 Select one or more SAPs, right-click, and choose Properties. The SAP configuration form opens with the General tab displayed.

7 Click on the Subscriber Management tab. The Host Connectivity tab is displayed.

8 Click on the Profiles tab.

9 Configure the Admin Status parameter by performing one of the following.

   a Set the parameter to Enabled to enable residential subscriber management on the SAP.

   b Set the parameter to Disabled to disable residential subscriber management on the SAP.

10 Click on the OK button. The SAP configuration form closes.

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The service configuration form closes.

13 Close the Manage Services form.

Procedure 65-25 To create a static host for residential subscriber management on a SAP

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a service and click on the Properties button. The service configuration form opens with the General tab displayed.

4 On the navigation tree, click on the site on which you want to create a static host for residential subscriber management on a SAP; expand the entries for that site.

5 Navigate to the SAPs that support subscriber management. Perform one of the following, depending on the type of service that you are configuring:

   a For an IES, the path is IES→Site→Subscriber Interfaces→*subscriber interface*→*group interface*→Service Access Points→*SAP*.

   b For a VPLS, the path is VPLS→Site→Access Interfaces→*SAP*.

   c For a VPRN service, the path is VPRN→Site→Subscriber Interfaces→*subscriber interface*→*group interface*→Service Access Points→*SAP*.

6 Select one or more SAPs, right-click, and choose Properties. The SAP configuration form opens with the General tab displayed.

7 Click on the Anti-Spoofing tab. The General tab is displayed.

8 Configure the Anti-Spoofing parameter.



Note — You must set the Anti-Spoofing parameter to IP-address matching or to IP- and MAC-address matching before you can enable subscriber management for the static hosts on a SAP.

9 Click on the Static Hosts tab.

10 Click on the Create button. The Access Interface Anti-Spoofing Static Host (Create) form opens with the General tab displayed.

11 Configure the parameters:

- IP Address
- MAC Address
- Subscriber Identification
- Use SAP ID as Subscriber ID
- ANCP String
- Intermediate Destination ID



Note — To enable residential subscriber management for a static host, you must specify values for the IP Address and Subscriber Identification parameters.

12 Configure the Administrative State parameter.

13 Click on the Select button in the Subscriber Profile panel to choose a subscriber profile for the static host, if required. The Select Subscriber Profile - AntiSpoofingStaticHosts form opens with a list of available subscriber profiles.



Note — To enable residential subscriber management for a static host, you must specify a subscriber profile.

14 Select a subscriber profile and click on the OK button. The Select Subscriber Profile - AntiSpoofingStaticHosts form closes, and the subscriber profile name appears in the Subscriber Profile panel.

15 Click on the Select button in the SLA Profile panel to choose an SLA profile for the static host, if required. The Select SLA Profile - AntiSpoofingStaticHosts form opens with a list of available SLA profiles.



Note — To enable residential subscriber management for a static host, you must specify an SLA profile.

16 Select an SLA profile and click on the OK button. The Select SLA Profile - AntiSpoofingStaticHosts form closes, and the SLA profile name appears in the SLA Profile panel.

17 Click on the Select button in the Application Profile panel to choose an application profile for the static host, if required. The Select Application Profile - AntiSpoofingStaticHosts form opens with a list of local application profiles.

18 Select an application profile and click on the OK button. The Select Application Profile - AntiSpoofingStaticHosts form closes, and the application profile name appears in the Application Profile panel.

19 Click on the OK button.



Note — The Administrative State parameter must be set to Up, to enable validation of Subscriber Identification, Subscriber Profile, and Application Profile.

Partially configured Static Hosts can be configured if the Administrative State parameter is set to Down.

20 Click on the Managed Routes tab.

21 Click on the Create button.

22 The Access Interface Anti-Spoofing Static Host Managed Route Display (Create)form opens.

23 Configure the parameters:

- IP Address
- Prefix Length

24 Click on the OK button. A dialog box appears.

25 Click on the OK button.The Access Interface Anti-Spoofing Static Host Managed Route Display (Create) form closes.

26 Click on the Apply button if you want to create an additional static host entry. A dialog box appears. Otherwise go to step 28.

27 Repeat steps 11 to 25 for each additional static host entry that you want to create.

28 Click on the OK button. A dialog box appears.

29 Click on the OK button. The Access Interface Anti-Spoofing Static Host (Create) form closes, and the SAP configuration form refreshes with the new static host entries.

30 Click on the OK button. The SAP configuration form closes.

31 Click on the OK button. A dialog box appears.

32 Click on the Yes button. The service configuration form closes.

33 Close the Manage Services form.

Procedure 65-26 To configure a MEP on a SAP

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a service and click on the Properties button. The service configuration form opens with the General tab displayed.

4 On the navigation tree, click on the site on which you want to configure a MEP on a SAP; expand the entries for that site.

5 Perform one of the following steps.

a To create a MEP on an Access Interface SAP, on the navigation tree, click on the site where you want to create the MEP; expand the entries for that site. Go to step 6

b To create a Down MEP on a Subscriber Group Interface SAP, on the navigation tree, click on the site where you want to create the Down MEP; expand the entries for that site. Go to step 7.



Note 1 — MEPs can be configured on an Access Interface SAP for VPLS, VPRN, IES, and VLL Epipe services.

Note 2 — Down MEPs can be configured on a Subscriber Group Interface SAP for VPRN and IES.

6 Click on the Access Interfaces icon to display the site SAPs. Go to step 8.

7 Click on the Group Interfaces icon to display the site SAPs.

8 Select one or more SAPs, right-click, and choose Properties. The SAP configuration form opens with the General tab displayed.

9 Click on the MEP tab.

10 Click on the Create button. The MEP (Create) form opens with the General tab displayed.

11 Configure the parameters:

- Auto-Assign ID
- ID
- Site ID
- Direction
- Administrative State
- CCM Messages Enabled
- Control MEP
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Propagation
- Type
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)
- CCM Padding Packet Size (Bytes)

The Control MEP parameter is only displayed if the Interface Type parameter is set to Ethernet Tunnel Path Endpoint.

The CCM Padding Packet Size (Bytes) parameter cannot be configured when the CCM interval parameter is set to 10 ms or 100 ms.



Note — When configuring a Down MEP on a Subscriber Group Interface SAP, the Direction parameter cannot be configured.

12 If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab. Otherwise, go to step 16.

13 Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

14 Click on the AIS tab.

15 Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

16 Click on the OK button. A dialog box appears.

17 Click on the OK button. The MEP (Create) form closes.

18 Close the Manage Services form.

Procedure 65-27 To list and manage subscriber management SAPs

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Select one of the available SAP types from the object drop-down list:

- IES Service Access Point (ies)
- L2 Access Interface (mvpls)
- L2 Access Interface (vpls)
- VPRN Service Access Point (vprn)

3 Click on the Select button to choose a site.

4 Click on the Search button. A list of SAPs for the selected service type appears.

5 To view or manage the information for a particular SAP, select the entry from the list and click on the Properties button. The SAP Properties form opens on the General tab. You can view SAP information or make changes to a variety of parameters on the various tabs of the form.

6 Click on the OK button to implement any changes you have made.

7 Close the Properties form.

8 Close the Manage Residential Subscribers form.

Procedure 65-28 To create a capture SAP

Perform this procedure to create a capture SAP, which enables MSAP creation.



Note 1 — A capture SAP does not carry traffic; the only purpose of a capture SAP is to trigger MSAP creation.

Note 2 — The created MSAPs are on the same port as the associated capture SAP.

Note 3 — A capture SAP must be the default SAP on a port.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services is displayed.

3 Select a VPLS in the list and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 In the navigation tree, expand the site to which you want to add the capture SAP.

5 Right-click on L2 Access Interfaces and choose Create VPLS L2 Access Interface. The VPLS L2 Access Interface (Create) form opens with the General tab displayed.

6 Set the SAP Sub Type parameter to Capture. The form displays a different array of tabs and panels.

7 Configure the remaining parameters:

- Description
- Administrative State

8 Use the Select button in the Host Lockout panel to choose a host lockout policy from the Select Policy form, if required.

9 Use the Select button in the Subscriber Authentication Policy panel to choose a subscriber authentication policy from the Select Subscriber Authentication Policy form, if required.

10 Click on the Port tab.

11 Use the Select button to choose a port from the Select Terminating Port form.

12 If required, configure the encapsulation values for the SAP. The encapsulation type of the terminating port determines the encapsulation values that are available. Table 65-4 describes the encapsulation values for each encapsulation type.

Table 65-4 Encapsulation types

Encapsulation type	Encapsulation values
dot1q	4095 only, which appears as an asterisk (*)
QinQ	1 to 4095 for the outer encapsulation value, and 4095 only for the inner encapsulation value
LAG	1 to 4095 for both encapsulation values

The capture SAP is used if a more specific match for the dot1q or QinQ tags is not found.



Note — Some providers use QinQ encapsulation to represent a service.sub or sub.service SAP. When configured, the full QinQ represents a subscriber.

13 To specify an ingress or egress queue group policy, perform the following steps.

i Click on the QoS tab.

ii Use the Select button in the Forwarding Plane Redirect panel to choose an ingress queue group template policy from the Select Forwarding Plane Queue Group Instance form.

iii Use the Select button in the Port Redirect panel to choose an egress queue group template policy from the Select Egress Queue Group Template Policy form.

14 To specify an ACL filter, perform the following steps.

i Click on the ACL tab.

ii Use the Select button to choose an ACL filter from the Select Ingress Filter form.

15 Click on the Security tab.

16 Click on the Select button in the NE DoS Protection panel to choose a DoS protection policy from the Select NE DoS Protection form, if required.

17 Perform one of the following.

a Configure the MAC Monitoring parameter.

b Configure the Ethernet CFM Monitor Flags parameter.

18 Use the Select button in the NE DDoS Protection panel to choose a DDoS protection policy from the Select NE DDoS Protection form, if required.

19 If the capture SAP is an ATM SAP, perform the following steps.

i Click on the ATM tab.

ii Configure the AAL5 Encapsulation parameter.

iii Click on the VC Ranges tab.

iv Click on the Create button. The ATM Configuration (Create) form opens.

v Configure the parameters:

- VC Range Index
- VPI Range Start
- VPI Range End
- VCI Range Start
- VCI Range End

vi Click on the OK button. A dialog box appears.

vii Click on the OK button. The ATM Configuration (Create) form closes.

20 Click on the Capture Access Interface tab.

21 Select one or more of the following parameters to specify the types of packets that are to trigger RADIUS authentication:

- DHCPv4 Trigger Packet
- PPP Trigger Packet
- PPPoE Trigger Packet
- ARP Trigger Packet
- DHCPv6 Trigger Packet



Note 1 — The PPP Trigger Packet parameter is selectable only on an ATM SAP.

Note 2 — The ARP Trigger Packet, DHCPv4 Trigger Packet and DHCPv6 Trigger Packet parameters are selectable only on a non-ATM SAP.

22 Use the Select button in the MSAP Defaults panel to choose an MSAP policy from the Select MSAP Policy form.

23 Configure the following parameters using the Select button for each, or by entering the values manually:

- MSAP Service ID
- MSAP Group Interface Name

24 Use the Select button beside the Policy parameter in the PPP panel to choose a PPP policy from the Select Policy form, if required.



Note — A PPP policy is selectable on only an ATM SAP.

25 Use the Select button beside the Policy parameter in the PPPoE panel to choose a PPPoE policy from the Select Policy form, if required.

26 Click on the Select button beside the Local User DB parameter in the following panels, as required, to choose a local user database for the protocol.

- PPP
- PPPoE
- DHCPv4
- DHCPv6



Note 1 — A PPP local user database is selectable on only an ATM SAP.

Note 2 — A DHCPv4 or DHCPv6 local user database is selectable on only a non-ATM SAP.

27 Use the Select button in the Redundancy panel to choose an SRRP instance from the Select SRRP Instance form.

28 Click on the OK button. A dialog box appears.

29 Click on the OK button. The VPLS L2 Access Interface (Create) form closes.

Procedure 65-29 To list MSAPs and view MSAP properties

Use this procedure to list MSAPs and view MSAP properties.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Choose Access Interface (Service Management) from the list.

3 Perform one of the following to display the MSAPs associated with each service:

- **a** For VPLS MSAPs:
  - **i** Click on the L2 Access Interface (Service Management).
  - **ii** Click on the Abstract L2 Access Interface (VPLS) icon.
  - **iii** Click on the L2 Access Interface (VPLS) icon.
  - **iv** Click on the VPLS L2 Access Interface icon.
  - **v** Choose VPLS MSAP and click on the Search button.
- **b** For IES MSAPs:
  - **i** Click on the Service Access Point icon (Service Management).
  - **ii** Click on the IES Service Access Point (IES) icon.
  - **iii** Choose IES MSAP and click on the Search button.
- **c** For VPRN MSAPs:
  - **i** Click on the Service Access Point icon (Service Management).
  - **ii** Click on the VPRN Service Access Point (VPRN) icon.
  - **iii** Choose VPRN MSAP and click on the Search button.

4 Choose an MSAP from the list and click on the MSAP Properties tab to view the MSAP properties.

Procedure 65-30 To view an MSAP event log, modify the global MSAP log policy, and purge MSAP log records

Use this procedure to view the event log for an MSAP, modify the global MSAP log policy, or purge the log records in an MSAP event log.

1 Perform Procedure 65-29 to list the MSAPs and choose the appropriate MSAP.

2 Click on the Events tab to display the MSAP event log.

3 If you need to view an event log record, choose a record from the event log and click on the Properties button. The Statistics Record - MSAP Event Log form opens and displays the MSAP record properties.

4 Close the Statistics Record - MSAP Event Log form.

5 If you need to modify the global MSAP event log policy click on the Log Policy button. The Log Policy - Ressubscr. MSap Event Log form opens.



Note — The global MSAP log policy affects all MSAP event logs.

6 Configure the parameters:

- Retention Time (hours)
- Administrative State

7 Click on the Apply button to save the changes.

8 Close the Log Policy - Ressubscr. MSap Event Log form.

9 If you need to purge the MSAP event log records, click on the Purge Log Records button.

10 Click on the OK or Cancel button to close the Log Policy - Ressubscr. MSap Event Log form.

11 Click on the Close button to close the Statistics Record - MSAP Event Log form.

Procedure 65-31 To modify and re-evaluate an MSAP policy on an MSAP

Use this procedure to re-apply an MSAP policy on an existing MSAP. MSAPs cannot be edited; however, MSAP policies on existing MSAPs can be changed and re-applied.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form appears.

2 Configure the filter criteria. See Procedure 65-29 for more information about configuring the filter to list MSAPs. A list of MSAPs for the service appears.

3 Choose an MSAP and click on the Properties button. The service configuration form opens with the General tab displayed.

4 Click on the MSAP Properties tab.

5 Click on the Properties button in the Creation MSAP Policy area and enter your required changes.

   i Click on the Apply button.

   ii Click on the OK button.

6 Click on the MSAP Properties tab.

7 Choose the Do Action option from the Creation MSAP Policy Re-evaluation parameter to apply the policies new parameter values. When you choose Not Applicable, the new parameter values in the policy are not applied but remain in the policy until you choose the Do Action option.

8 Click on the Apply button.

9 Click on the OK button.

Procedure 65-32 To modify an MSAP policy and re-evaluate the MSAPs

Use this procedure to re-apply an MSAP policy on existing MSAPs. MSAPs cannot be edited; however, MSAP policies on existing MSAPs can be changed and re-applied.

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form appears.

2 Choose the policy scope as required. The policy scope can be Global or Local.

3 Configure the filter criteria to list MSAPs for the service. Choose MSAP Policy (MSAP Policy) and click on the Search button. A list of MSAP policies appears in the form.

4 Choose an MSAP policy and click on the Properties button. The MSAP Policy (Edit) form appears with the General tab displayed.

5 Enter your required changes.

   i Click on the Apply button.

   ii Click on the OK button.

6 Click on the Reevaluate MSAPs button. The MSAPs are re-evaluated with the changed MSAP policy.

7 Click on the Apply button.

8 Click on the OK button.

Procedure 65-33 To re-evaluate lease states for an MSAP

Use this procedure to push SLA profile or subscriber profile changes out to an MSAP. MSAPs cannot be edited; however, SLA profiles or subscriber profiles on existing default SAPs can be changed and re-applied. The Re-evaluate Lease States command updates all residential subscriber hosts associated with the MSAP without reinstantiating the hosts.



Note — This procedure describes how to perform a Re-evaluate Lease States function from a residential subscriber GUI context. The same function can be performed from an IES or VPRN group interface GUI context.

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Configure the filter criteria to list IES or VPRN SAPs. Choose IES Service Access Point or VPRN Service Access Point from the drop-down list.

3 Click on the Select button next to the Site ID field.

4 Choose the IES or VPRN site on which you want to perform a Re-evaluate Lease States function from the Select An ESM Capable Network Element form and click OK.

5 In the Manage Residential Subscribers form, click on the Search button. A list of applicable SAPs appears in the form.

6 Click on a SAP from the list and click on the Re-evaluate Lease States button.

An information window appears, indicating the number of hosts that were sent a Re-evaluate Lease Sates request, and the number of hosts that were skipped. Click OK to close the window.

7 Close the Manage Residential Subscribers form.

Procedure 65-34 To delete an MSAP

Use this procedure to delete any MSAP that is an inactive state. Verify that the MSAP is in an inactive state. The 5620 SAM prevents attempts to delete an MSAP that is in an active state.

1 Perform Procedure 65-29 to list the MSAPs and choose the appropriate MSAP to delete.

2 Click on the Delete button. A dialog box appears.

3 Click on the Yes button in the dialog box. The MSAP is deleted.

Procedure 65-35 To delete an MSAP policy

Use this procedure to delete any MSAP policy on an MSAP that is an inactive state. Ensure that the MSAP is inactive and that the policy is not associated with other MSAPs that may be used at a later date. Do not attempt to delete MSAP policies on MSAPs that are in an active state.

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Residential Subscriber form appears.

2 In the Manage Residential Subscriber form, choose the Policy scope.

3 Choose MSAP Policy (MSAP Policy) from the list.

4 Click on the Search button in the Manage Residential Subscriber form. The MSAP policies are listed in the MSAP Policy list form.

5 Choose one or more MSAP policies that you need to delete.

6 Click on the Delete button. A dialog box appears.

7 Click on the Yes button in the dialog box. The MSAP policy is deleted.

Procedure 65-36 To configure DHCP event monitoring for a SAP

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Select one of the available SAP types from the object drop-down list:

- IES Service Access Point (ies)
- L2 Access Interface (mvpls)
- L2 Access Interface (vpls)
- VPRN Service Access Point (vprn)

3 Click on the Select button to choose a site.

4 Click on the Search button. A list of SAPs appears.

5 To configure DHCP monitoring for a particular SAP, select the entry from the list and click on the Create Monitored SAP button. The Monitored Access Interface (Create) form opens with the General tab displayed.

Note — A maximum of five hosts or five SAPs can be monitored simultaneously. If more than the maximum number of hosts is selected and configured for monitoring an error message will be displayed.

6 Configure the parameters:

- Monitoring Period
- Units

7 Click on the OK button to close the Monitored Access Interface (Create) form.

Note — You must complete Procedure 65-37 to enable and schedule SAP monitoring.

8 Close the Manage Residential Subscribers form.

Procedure 65-37 To monitor DHCP events for a SAP

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Monitored Access Interface from the object drop-down list.

3 Configure the filter criteria at the top-right panel of the form, if required.

4 Click on the Search button. A list of Monitored SAPs appears.

5 To initiate or view DHCP monitoring for a particular SAP, select the entry from the list and click on the Properties button. The Monitored Access Interface (Edit) form opens on the General tab.

6 You can perform one or more of the following on this form:

a To start monitoring the chosen SAP, click on the Start Monitor button.

b To stop monitoring the chosen SAP, click on the Stop Monitor button.

c To remove monitoring of the chosen SAP, click on the Delete button.

d To change the Monitoring Period, click on the Stop Monitor button, enter the desired value into the field, and select an appropriate Unit from the adjacent drop-down menu.

7 To view DHCP events for the chosen SAP, click on the Events tab. The DHCP Events list is displayed. The 5620 SAM supports monitoring of the following DHCP events:

- DHCP Lease Entries Exceeded
- DHCP Lease State Overriden
- Suspicious DHCP Packet
- DHCP ACK Dropped
- Host Connectivity Lost
- Host Connectivity Restored

8 Select an event from the list and click on the Properties button to view detailed information about the event.

9 Click on the OK button to close the Monitored Access Interface form.

10 Close the Manage Residential Subscribers form.

Procedure 65-38 To view or configure active residential subscriber hosts on a SAP



Note — The 5620 SAM does not automatically display a list of all active hosts on a SAP because the number of hosts on a SAP is potentially large and may take a long time to retrieve. You must request the list of hosts on a SAP. The 5620 SAM prompts you for confirmation before retrieving the list of hosts.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a service and click on the Properties button. The service configuration form opens with the General tab displayed.

4 On the navigation tree, click on the site on which you want to view or configure active residential subscriber hosts on a SAP; expand the entries for that site.

5 Click on the Access Interfaces icon to display the site SAPs.

6 Select a SAP, right-click, and choose Properties. The SAP configuration (Edit) form opens with the General tab displayed.

7 Click on the Subscriber Management tab. The Host Connectivity tab is displayed.

8 Click on the Subscriber Hosts tab.

9 Click on the Find button. A confirmation prompt appears.

10 Click on the Yes button. The list of subscriber hosts refreshes with the active subscriber host entries.

11 To view the information for a subscriber host, select the host entry and click on the Properties button. The Subscriber Host form opens with the subscriber host information displayed.

12 If the subscriber host is a static host, go to step 20.

13 Configure the Subscriber Profile String parameter for the dynamic host or PPPoE host, if required. Click on the Select button to choose a subscriber profile string from the Subscriber Profile String - Subscriber Host form, or simply type a subscriber profile string in the field.



Caution — Changing the subscriber profile string directly on a subscriber host is potentially service-affecting to all hosts on all SAPs that belong to the subscriber. Because a subscriber is associated with only one subscriber profile, when you change the subscriber profile string for one host, all dynamic or PPPoE hosts associated with the subscriber on all SAPs are automatically configured with the new subscriber profile.

14 Configure the SLA Profile String parameter for the dynamic host or PPPoE host, if required. Click on the Select button to choose an SLA profile from the SLA Profile - Subscriber Host form, or simply type an SLA profile string in the field.

15 Configure the ANCP String and Intermediate Destination ID parameters, if required.

16 Configure the Application Profile parameter for the dynamic host PPPoE host, if required. Click on the Select button to choose an application profile string from the Application Profile String - Subscriber Host form, or simply type an application profile string in the field.



Caution — Changing the application profile string directly on a subscriber host is potentially service-affecting to all hosts on all SAPs that belong to the subscriber. Because a subscriber is associated with only one application profile, when you change the application profile string for one host, all dynamic or PPPoE hosts associated with the subscriber on all SAPs are automatically configured with the new application profile.

17 Click on the OK button. A dialog box appears.

18 Click on the Yes button. The Subscriber Host form closes.

19 Go to step 21.

20 Click on the Cancel button to close the Subscriber Host form.

21 Click on the OK button. The SAP configuration form closes.

22 Close the Manage Services form.

66 — VLAN service management

66.1 VLAN service management overview *66-2*

66.2 Sample L2 VPN VLAN configuration *66-6*

66.3 Sample BTV VLAN configuration *66-8*

66.4 Sample interconnection VLAN configuration *66-10*

66.5 Workflow to create VLAN services (OmniSwitch) *66-12*

66.6 VLAN service management procedures *66-14*

66.1 VLAN service management overview

VLANs are created to provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address issues such as scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic flow management. Table 66-1 lists the types of VLAN services that are supported on the 5620 SAM by device type:

Table 66-1 Device VLAN support

Device	Supported VLAN types
7450 ESS	• Standard VLAN • L2 VPN (TLS/VLAN-Stacking) VLAN • Broadcast TV (MVR/IPMV) VLAN
All OmniSwitches	• Standard VLAN • L2 VPN (TLS/VLAN-Stacking) VLAN
All OmniSwitches except for the OS 6900 and OS 10K	• Broadcast TV (MVR/IPMV) VLAN
OS 6900 and OS 10K	• IPC VLAN • VIP VLAN
9500 MPR (1)	• 9500 MPR (dot1ad) VLAN • 9500 MPR P2P (dot1q) VLAN • 9500 MPR P2MP (dot1q) VLAN

Note

(1) See “9500 MPR VLAN service management” in the *5620 SAM MPR User Guide* for VLAN service management configuration information.

Several 7450 ESS, 9500 MPR and OmniSwitch VLAN services can be interconnected through a backbone VPLS.

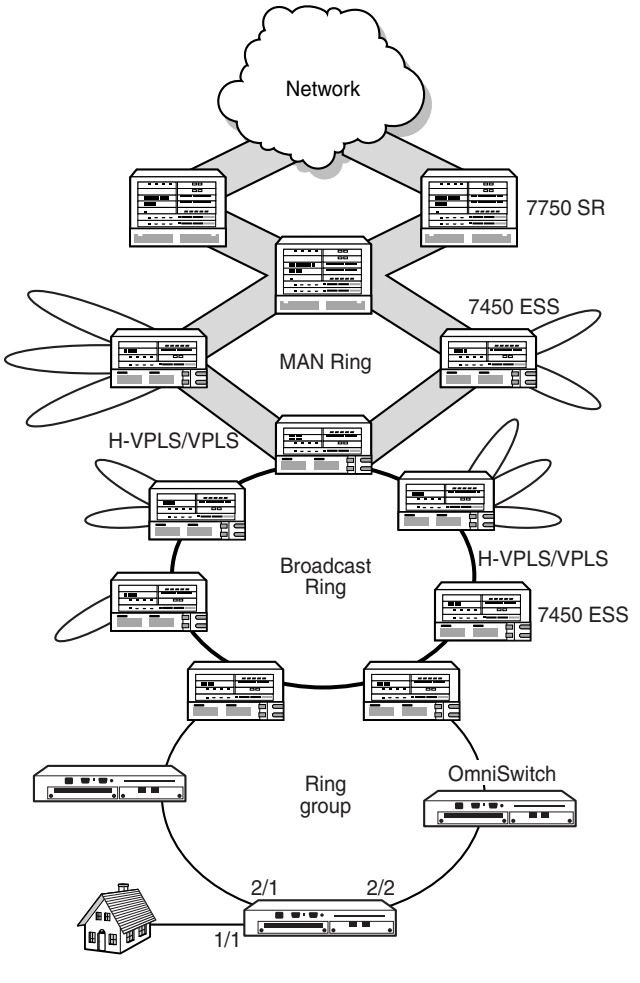
The 5620 SAM supports end-to-end VLAN configuration using the following methods:

- Tabbed configuration forms with an embedded navigation tree. The navigation tree provides a logical view of the service and acts as a configuration interface.
- Pre-configured template. A user who is assigned the template management role can create a service template. See “Managing templates” in the *5620 SAM Scripts and Templates Developer Guide* for more information about the administrative tasks associated with service templates.

VLAN ring groups

VLAN ring groups are used to send traffic across an Ethernet ring using copper or fiber optic connections from the source traffic device, for example, from a 7450 ESS, to all devices in the ring. STP configuration on OmniSwitch devices ensures that there is a constant stream of traffic in either direction by rerouting traffic around breaks in the physical links between the devices. Figure 66-1 shows an example of a ring group that is part of a larger metropolitan area network.

Figure 66-1 Ring in a metropolitan and broadcast network



The 5620 SAM provides OAM tools for service validation and for troubleshooting service and network transport issues.You can run the OAM Validation test suite for the VLAN service by clicking on the Validate button or by clicking on the More Actions button and choosing Validate. Alternatively, you can also perform a One Time Validation. If a check mark appears beside the OAM Validation Failed state cause indicator, the test has failed. In addition, the Tested Entity Result tab on the Tests tab displays more detailed information about the OAM test result. See chapter 77 for more information about how to configure OAM validation test suites.

The Aggregated Service Site Operational State parameter has four possible values. The value is derived from the operational states of the sites that are part of the service, as follows:

- Up—all sites are operationally up
- Partially Down—at least one site is operationally down
- Down—all sites are operationally down
- Unknown—the service has no provisioned sites

When the Aggregated Service Site Operational State parameter is Partially Down or Down, a check mark appears beside the appropriate State Cause indicator to identify the type of fault to the 5620 SAM operator. You can view alarms on the Faults page.

When you use the 5620 SAM to create or discover a service, the 5620 SAM assigns a default tier value to the service. The Service Tier parameter value is relevant only in the context of composite service topology map views. See chapter 74 for more information about the hierarchical organization of composite services.

VLAN groups

The 5620 SAM supports the configuration and provisioning of VLAN groups which are used by the following NEs.

- OmniSwitch devices to configure VLAN services
- 9500 MPR ANSI/ETSI (2.x and 3.x streams) to configure VLAN and VLL services

You can use VLAN groups to:

- logically group OmniSwitch and 9500 MPR devices to represent a typical network topology. An OmniSwitch and a 9500 MPR cannot belong to the same VLAN group.
- manage the VLAN IDs that are assigned to 9500 MPR VLAN group members.

See Procedure 66-6 for more information about creating VLAN groups for OmniSwitch devices. See “9500 MPR VLAN service management” in the *5620 SAM MPR User Guide* for more information about creating VLAN groups for 9500 MPR/9500 MPRe devices.

OmniSwitch VLAN service policies

Policies can be assigned to ports on an OmniSwitch. Policies are defined at a global level and then applied to components of the service, such as a port.

The policy on the component is then a local version of the global policy. The following policies are common to VLAN services:

- QoS policies define ingress classification, policing, shaping, and marking on the device.
- UNI policies define how control frames that are received on a port are processed. UNI policies are applied to a port that is used as a SAP in a L2 VPN TLS (stacked) VLAN.
- SAP policies define traffic engineering parameters for bandwidth sharing, rate limiting, CVLAN translation (or double-tagging), and priority bit mapping. SAP policies are applied to the service access multi-point.
- Filter policies control network traffic into or out of an interface or device based on IP or MAC matching criteria.

See chapter 42 for more information about policies.

OmniSwitch network management

The 5620 SAM manages OmniSwitch devices using SNMP and CLI messages. OmniSwitch devices support termination of all VLAN types on Ethernet ports.

Spanning tree protocols

The STP configuration on an OmniSwitch device in a VLAN group detects loops in the topology and ensures that there is a constant stream of traffic by rerouting traffic around breaks in the physical links between the devices. OmniSwitch devices support STP, MSTP and RSTP.

STP

STP is a Layer 2 link management protocol that provides path redundancy while preventing undesirable loops in the network. Fault-tolerant internetworks must have a loop-free path between all the nodes in a network. The spanning tree algorithm calculates the best loop-free path through a switched Layer 2 network. Switches send and receive STP frames at regular intervals but do not forward these frames.

See the OmniSwitch user documentation for more information about STP CLI commands and parameters and Spanning Tree modes.

The OmniSwitch can operate in the following spanning tree modes:

- flat
- 1 x 1

The flat mode provides a CST instance that applies across all VLANs and supports STP (802.1D), RSTP (802.1w), and MSTP. MSTP allows the mapping of one or more VLANs to a single spanning tree instance.

The 1x1 mode is an Alcatel-Lucent proprietary implementation that automatically calculates a separate spanning tree instance for each VLAN configured on the switch. This mode only supports the use of the STP and RSTP.

By default, an OmniSwitch runs in the 1x1 mode and uses the 802.1D protocol.

The 5620 SAM supports the configuration of Spanning Tree protocols and modes.

RSTP

RSTP uses point-to-point wiring to provide rapid convergence of the spanning tree. With RSTP, the spanning tree may be reconfigured in less than 1 s, as compared to 50 s required with the default STP settings. This is critical in networks that carry voice, video, and other delay-sensitive traffic.

RSTP assigns port roles and determines the active topology to provide rapid convergence of the spanning tree. RSTP selects the switch with the highest switch priority.

See the OmniSwitch user documentation for more information about RSTP CLI commands and parameters.

MSTP

MSTP allows you to group and associate VLANs to multiple spanning tree instances, or forwarding paths. MSTP allows up to 16 RSTP instances to be run and associates a VLAN with a specific MST instance. This reduces link convergence time and enables load balancing over a large number of VLANs.

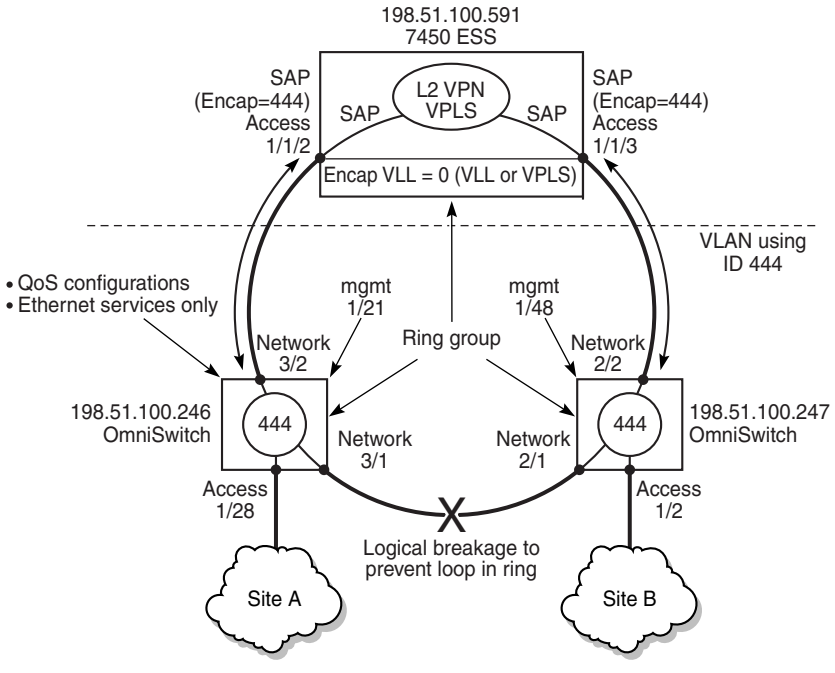
Each MST instance can have its own independent topology. Multiple forwarding paths improve network fault tolerance because when one instance fails, data flow is unaffected over the remaining forwarding paths. You can manage large networks and use redundant paths more easily by allocating different VLAN and spanning tree instance assignments to different parts of the network.

See the OmniSwitch user documentation for more information about RSTP CLI commands and parameters.

66.2 Sample L2 VPN VLAN configuration

Figure 66-2 shows a sample L2 VPN VLAN service configuration. Transparent LAN services such as a L2 VPN are used to transport large numbers of customer VLANs while keeping the traffic in each VLAN segregated. The configuration depends on the specific network requirements.

Figure 66-2 Sample L2 VPN VLAN configuration



Verify that the following preconfigurations are complete.

- Ensure that the appropriate preconfigurations have been performed on the OmniSwitch devices.
  - pre-discovery CLI modifications
  - discovery including mediation configuration with the CLI user names and passwords
  - configure protocol to manage topology loops, such as MSTP or RSTP
- Ensure that the VPLS that feeds the ring VLAN service is configured on the 7450 ESSs. The encapsulation of the SAPs that belong to the VPLS on the 7450 ESSs must match the VLAN ID of the ring VLAN.
- Configure the OmniSwitch ports as access (ports that are part of the VLAN) and network (ports that are used for uplinks), as required, from the navigation tree.
- Devices that belong to the ring, and the 7450 ESS that the ring connects to, should be added to the ring group.
- Ensure that the appropriate preconfigurations have been performed on the 7450 ESS.
  - A VLL is created with 0 encapsulation between the SAPs (1/1/2 and 1/1/3) on the 7450 ESS
  - The SAPs on the 7450 ESS that are part of the VPLS use the same encapsulation as the VLAN ID for the ring group
  - A L2 VPN VPLS is created on the 7450 ESS.



Note — Only Ethernet services are supported on an OmniSwitch L2 VPN VLAN service.

Table 66-2 lists the high-level tasks that are required to configure this sample VLAN L2 VPN service.

Table 66-2 Sample VLAN L2 VPN service configuration

Task	Description
1. Manage and configure devices	Ensure that the required configurations are completed to equipment, including configuring access and network ports, enabling CLI configuration on managed OmniSwitch devices: • The ring group contains all three devices. • Ports 3/1 and 3/2 on the device connected to Site A and 2/1 and 2/2 connected to Site B are configured as network to act as uplinks. • Ports 1/1/2 and 1/1/3 are configured as access on the 7450 ESS, and the encapsulation matches the VLAN ID (444). • Ports 1/2 and 1/28 on the OmniSwitch devices are configured as access ports.
2. Configure policies as required	Policies should be configured before you create a service. The following key policies can be applied to resources that are part of a VLAN. • QoS policies for the OmniSwitch devices and ports • scheduling policies • filter policies, including IGMP filter policies to create and deploy access control lists on the OmniSwitch devices in the ring
3. Distribute policies to devices	Distribute configured policies to the devices. The policies are used during the creation of VLAN services.

(1 of 2)

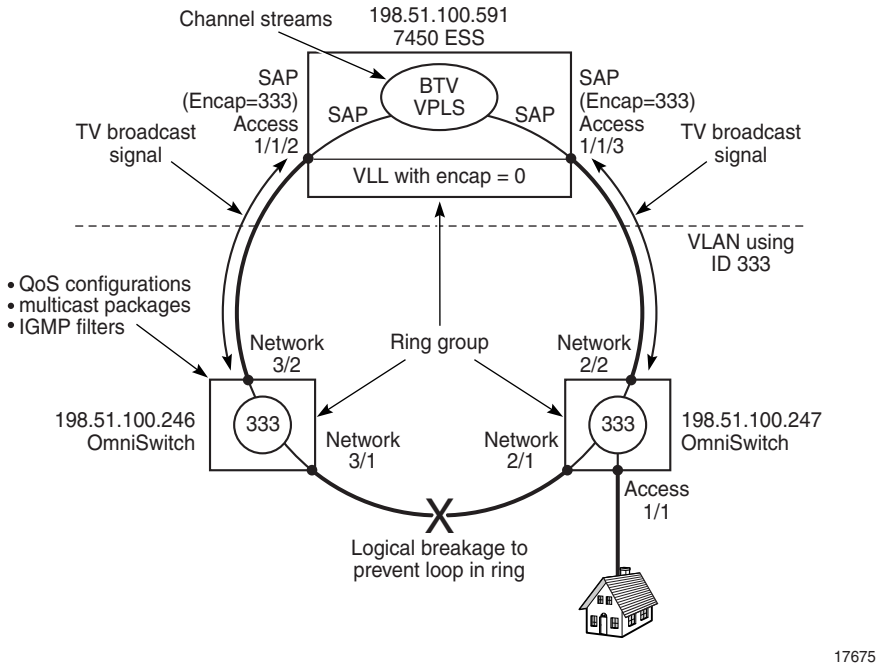
Task	Description
4. Create VLAN services	Create VLAN services using a series of configuration forms. Ensure that the VLAN created for the ring group uses ID 444.
5. Add access interfaces	Associate access interfaces (similar to SAPs) with VLAN services, that are the physical ports to which end users connect. Use the L2 Interfaces tab on the VLAN properties form to associate VLAN services with the ports used by end users.

(2 of 2)

66.3 Sample BTV VLAN configuration

Figure 66-3 shows a sample broadcast TV VLAN configuration. BTV VLANs are shared VLANs, where the multicast broadcast channels or pay per view channels are available across the ring, and based on subscriptions and privileges determined using IGMP snooping, the user gains or is denied access. The configuration depends on the specific network requirements.

Figure 66-3 Sample BTV VLAN configuration



Verify that the following preconfigurations are complete.

- Ensure that the appropriate preconfigurations have been performed on the OmniSwitch devices:
  - pre-discovery CLI modifications
  - SNMP trap forwarding to the 5620 SAM
  - discovery, including mediation configuration with the CLI user names and passwords
  - configure protocols to manage topology loops, such as MSTP or RSTP

- Ensure that the BTV VPLS that feeds the ring VLAN service is configured on the 7450 ESSs. The encapsulation of the SAPs that belong to the VPLS on the 7450 ESSs should match the VLAN ID of the ring VLAN.
- Configure OmniSwitch ports as access (ports that are part of the VLAN) and network (ports that are used for uplinks), as required, from the navigation tree.
- OmniSwitch devices that belong to the ring, and the 7450 ESS that the ring connects to, should be added to the ring group.
- Ensure that the appropriate preconfigurations have been performed on the 7450 ESS.
  - A VLL is created with 0 encapsulation between the SAPs (1/1/2 and 1/1/3) on the 7450 ESS
  - The SAPs on the 7450 ESS that are part of the VPLS use the same encapsulation as the VLAN ID for the ring group
  - A BTV VPLS is created on the 7450 ESS.
- Create and manage the necessary broadcast TV policies, including multicast package and IGMP filtering.

Table 66-3 lists the high-level tasks that are required to configure this sample broadcast TV VLAN service.

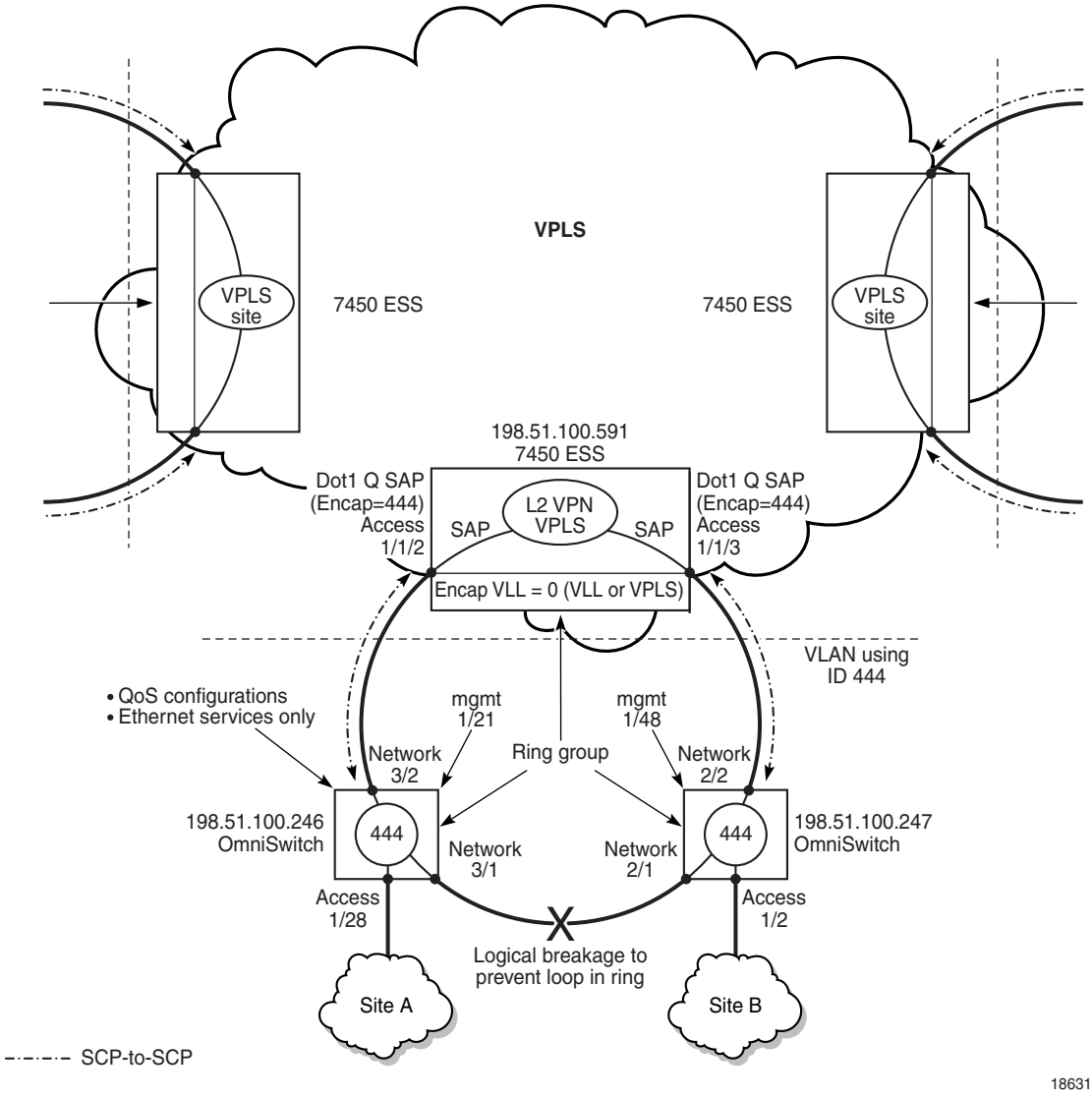
Table 66-3 Sample broadcast TV VLAN service configuration

Task	Description
1. Manage and configure devices	Ensure that the required configurations are completed to equipment, including configuring access and network ports, enabling CLI configuration on managed OmniSwitch devices, and the creation of ring groups: • The ring group contains all three devices. • Ports 3/1 and 3/2 on the device with the IP address 198.51.100.246 and ports 2/1 and 2/2 on the device with the IP address 198.51.100.247 are configured as network to act as uplinks. • Ports 1/1/2 and 1/1/3 are configured as access on the 7450 ESS with an encapsulation matching the VLAN ID (333). • Port 1/1 on device 192.168.200.247 is configured as access.
2. Configure policies as required	Policies should be configured before you create a service. The following key policies can be applied to resources that are part of a VLAN BTV service. • QoS policies for OmniSwitch devices and ports • scheduling policies • filter policies, including IGMP filter policies to create and deploy access control lists on the OmniSwitch devices in the ring • multicast package policies to determine the content of the broadcast streams that are sent to the OmniSwitch devices in the ring
3. Distribute policies to devices	Distribute configured policies to the devices. Policies are used during the creation of VLAN services.
4. Create VLAN services	Create VLAN services using a series of configuration forms: Ensure that the VLAN created for the ring group uses ID 333.
5. Add access interfaces	Associate access interfaces (similar to SAPs) with VLAN services, that are the physical ports to which end users connect. You use the L2 Interfaces tab on the VLAN properties form to associate VLAN services with the ports used by end users.

66.4 Sample interconnection VLAN configuration

Figure 66-4 shows a sample configuration of an interconnection of VLANs across a VPLS backbone.

Figure 66-4 Sample interconnection VLAN



Verify that the following preconfigurations are complete:

- Ensure that the appropriate preconfigurations have been performed on the OmniSwitch devices.
  - pre-discovery CLI modifications
  - SNMP trap forwarding to the 5620 SAM
  - discovery including mediation configuration with the CLI user names and passwords
  - ports are configured as access (ports that are part of the VLAN) and network (ports that are used for uplinks)
  - configure protocol to manage topology loops, such as MSTP or RSTP, using CLI
- Configure OmniSwitch ports as access and network, as required, from the navigation tree.
- OmniSwitch devices that belong to the ring, and the 7450 ESS that the ring connects to, should be added to the ring group.

Table 66-4 lists the high-level tasks that are required to configure this sample interconnection of VLAN services.

Table 66-4 Sample VLAN interconnection configuration

Task	Description
1. Manage and configure	Ensure that the required configurations are completed to equipment as described in Table 66-2, including the following. • configuring access and network ports • enabling CLI configuration on managed OmniSwitch devices • configuring and distributing policies
2. Create VLAN services	Create VLAN services using a series of configuration forms. Ensure that the VLAN created for the ring group uses ID 444.
3. Configure VPLS	Ensure that the encapsulation value of the ports that contain the SAPs on the 7450 ESS matches the VLAN ID of each VLAN service in the ring group. Ensure that the encapsulation value of the ports that contain the SAPs on the 7450 ESS at each VPLS site is Dot1 Q. See chapter 68 for more information about creating a VPLS.
4. Create composite service	Create a composite service to interconnect the VLAN services with the VPLS. • Create the composite service. • Define general properties for the composite service. • Specify the services that are participating in the composite service. You can specify multiple services in one operation. • Create SCP-to-SCP connectors to link the dot1q-encapsulated VPLS SAP and the adjacent L2 switch uplinks of the VLAN ring group. See chapter 74 for more information about creating composite services.

66.5 Workflow to create VLAN services (OmniSwitch)

The following workflow lists the high-level steps required to create a VLAN service on OmniSwitch devices. As a prerequisite for creating a VLAN service, this workflow assumes that the following appropriate preconfigurations have been performed:

- pre-discovery CLI modifications
- discovery including mediation configuration with CLI usernames and passwords
- addition of the OmniSwitches that participate in the VLAN to a VLAN group
- configure OmniSwitch network ports, as required, from the navigation tree. The Automatic VLAN Binding parameter associated with a network port or LAG must be enabled before the 5620 SAM can identify the network port or LAG as a network interface. This parameter is only supported on Stacked VLANs.
- configure QoS policies, as required.
- set up customers or associate existing customers with the new service; see "5620 SAM user security tasks" in the *5620 SAM System Administrator Guide* for more information.

1 Provision a Standard VLAN service. See Procedure 66-1.

i Create the VLAN and associate a customer with the VLAN. Set the application parameter to Standard VLAN.

ii Add sites that are participating in this VLAN. Configure STP and VLAN properties, as required.

iii Create VLAN access interfaces to be used for this service. Specify the access port to be used by each interface and whether the access is tagged.

2 Provision a L2 VPN VLAN service. See Procedure 66-2.

i Create the VLAN and associate a customer with the VLAN. Set the application parameter to L2-VPN (TLS/VLAN-Stacking).

ii Add devices connected as part of a VLAN group to the VLAN.

iii Add sites that are participating in this VLAN. Configure STP and VLAN properties, as required.

iv Create Ethernet services. Enter the names of the services that you need to associate with the SVLAN created in the previous steps.

v Create one or more service access multipoints. SAPs, CVLANs, and a SAP policy are associated with a service access multipoint. A service access multipoint is assigned a user-selected or auto-generated ID when the multipoint is created.

vi Create SAPs. Specify the port to be used as a customer-facing port (UNI).

vii Create CVLANs to associate customer traffic with a VLAN-stacking SAP. CVLANs identify the type of customer traffic that is received on the SAP UNI ports.

3 Provision a BTV VLAN service. See Procedure 66-3.

i Create the VLAN and associate a customer with the VLAN. Set the application parameter to Broadcast TV (MVR/IPMV).

ii Add devices connected as part of a VLAN group, to the VLAN.

iii Create an L2 access interface. The interface acts as the receiver port on the IPMV. The port that is selected must already be used as a SAP in a SVLAN.

iv Create Ethernet services. Enter the names of the services that you need to associate with the SVLAN created in the previous steps.

v Create one or more service access multipoints. SAPs, CVLANs, and a SAP policy are associated with a service access multipoint. A service access multipoint is assigned a user-selected or auto-generated ID when the multipoint is created.

vi Create SAPs. Specify the port to be used as a customer-facing port (UNI). The UNI port must already be configured as a receiver port on the IP multicast VLAN.

vii Create CVLANs that will be used to associate customer traffic with a VLAN stacking SAP. CVLANs identify the type of customer traffic received on the SAP UNI ports. The service processes and tunnels the traffic through the SVLAN.

viii Add multicast group addresses to the IP multicast VLAN site.

ix Add CVLAN tags to the IP multicast VLAN site. CVLAN tags are used to bind IP multicast VLANs to a receiver port.

4 Provision a VIP VLAN service. See Procedure 66-4.

5 Associate access interfaces (similar to SAPs) with the VLAN services. These are the physical ports to which end users connect. Use the L2 Interfaces tab on the VLAN properties form to associate VLAN services with the ports used by end users. See Procedure 66-5.

6 For services created on a OmniSwitch, as required:

a Create VLAN groups and add members to each group as required. See Procedure 66-6.

b Delete a VLAN group or group member. See Procedure 66-7.

c Add a MEP to an OmniSwitch VLAN service access interface. See Procedure 66-8.

d Configure IGMP on an OmniSwitch VLAN site. See Procedure 66-9.

7 Turn up the service.

Network interface VLAN bindings are created between the newly-created VLAN and all of the network ports on the node.

8 As required, run an OAM validation test on a VLAN service. See Procedure 66-10.

9 As required, view VLAN information:

a View the VLAN service operational status. See Procedure 66-11.

b View the service topology map associated with a VLAN service. See Procedure 66-12.

10 As required, modify a VLAN service. See Procedure 66-13.

11 As required, delete a VLAN service. See Procedure 66-14.

66.6 VLAN service management procedures

Use the following procedures to perform VLAN creation and management tasks.

Procedure 66-1 To create a standard VLAN service

Perform the following procedure to create a standard VLAN service on OmniSwitch devices.



Note — Alcatel-Lucent recommends that you specify the OmniSwitch ports that will be network interfaces before you configure a standard VLAN service.

1 Choose Create→Service→VLAN from the 5620 SAM main menu. The VLAN (Create) Service form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the VLAN. The Select Customer - VLAN Service form opens.

3 Select a customer for the VLAN and click on the OK button. The Select Customer - VLAN Service form closes and the VLAN Service (Create) form reappears with the customer information displayed in the General tab.

4 Configure the parameters:

- Service ID
- Auto-Assign ID
- SVC Mgr Service ID
- Service Name
- Description
- Service Tier
- Service Priority
- Administrative State
- Current OLC State
- Revert OLC State

The Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.

The SVC Mgr Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.

The Current OLC State parameter is configurable when you click on the Apply button on the VLAN Service (Create) form.

5 Click on the VLAN tab.

6 Set the Application parameter to Standard VLAN.

7 Click on the Select button in the Group panel to choose a group to associate with the VLAN. The Select Group - VLAN Service form opens.

8 Select a group and click on the OK button. The Select Group - VLAN Service form closes and the VLAN (Create) form reappears with the group information displayed.

9 On the navigation tree, right-click on VLAN and choose Create VLAN Site. The Select Network Elements - VLAN form opens.

10 Select a site and click on the OK button. The Select Network Elements - VLAN form closes and the Site (Create) form appears with the site information displayed on the General tab.

11 Configure the parameters.

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State

12 Click on the VLAN tab.

13 Configure the parameters:

- Enable Mobile-Tag
- Enable Authentication

14 On the navigation tree, right-click on L2 Access Interfaces and choose Create VLAN Access Interface. The VLAN Access Interface (Create) form opens with the General tab displayed.

15 Configure the parameters.

- Description
- Administrative State

16 Click on the Port tab.

17 Click on the Select button to choose a port for the VLAN access interface. The Select Terminating Port - VLAN Access Interface form opens.



Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

18 Use the configurable filter and Search button to choose a port for user-side access to the VLAN, and click on the OK button. The Select Terminating Port - VLAN Access Interface form closes, and the VLAN Access Interface (Create) form displays the port information.

19 Click on the VLAN tab.

20 Configure the VLAN Tagging parameter. The parameter must be set to Tagged on CES interfaces.

You can only configure this parameter when you create a SAP. After the SAP is created, the parameter cannot be modified. If you need to change the value of this parameter, you must first delete the SAP and create a SAP that matches the new requirements.

21 Click on the OK button. The VLAN Access Interface (Create) form closes, and a dialog box appears.

22 Click on the OK button. The Site (Create) form reappears.

23 Repeat steps 14 to 22 for each access interface that you need to create on the site.

24 Click on the DHCP Snooping tab if you need to enable DHCP snooping on the VLAN. The DHCP Snooping General tab appears.

25 Click on the Create button. The VLAN Level DHCP Snooping (Create) form opens.

26 Configure the parameters:

- VLAN Level Option-82 Data Insertion
- VLAN Level MAC Address Verification

These parameters are automatically enabled when DHCP snooping is enabled on a VLAN.

27 Click on the OK button. The VLAN Level DHCP Snooping (Create) form closes, and a dialog box appears.

28 Click on the OK button. The DHCP Snooping General tab reappears.

29 Click on the Binding Database tab if you need to add a static entry to the DHCP binding table.

30 Click on the Create button. The DHCP Snooping Binding Database (Create) form opens.

31 Configure the MAC Address parameter.

32 Click on the Select button to choose a port. The Select Port - DHCP Snooping Binding Database form opens.

33 Choose a port from the list and click on the OK button.

34 The DHCP Snooping Binding Database (Create) form reappears.

35 Configure the parameters:

- IP Address
- Lease Time

36 Click Apply to add the static entry to the table. A dialog box appears.

37 Click on the OK button.

38 Repeat steps 29 to 37 for each static entry that you need to add to the binding table.

39 Click the Cancel button to close the DHCP Snooping Binding Database (Create) form.

40 Click on the OK button. The Site (Create) form reappears.

41 Click on the OK button. The VLAN (Create) form reappears with the new site information displayed.

42 Click on the OK button to close the VLAN (Create) form.

Procedure 66-2 To create an OmniSwitch L2 VPN TLS VLAN service



Note 1 — The TLS Mode must be set to Ethernet Service before a sL2 VPN TLS (stacked) VLAN service can be created on an OmniSwitch. See Procedure 23-63 to configure the TLS Mode.

Note 2 — Alcatel-Lucent recommends that you configure OmniSwitch network ports before you configure a L2 VPN TLS VLAN service.

1 Choose Create→Service→VLAN from the 5620 SAM main menu. The VLAN Service (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the L2 VPN TLS VLAN. The Select Customer - VLAN Service form opens.

3 Select a customer for the L2 VPN and click on the OK button. The Select Customer - VLAN Service form closes and the VLAN Service (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters:

- Service ID
- Auto-Assign ID
- SVC Mgr Service ID
- Service Name
- Description
- Service Tier
- Service Priority
- Administrative State
- Current OLC State
- Revert OLC State

The Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.

The SVC Mgr Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.

The Current OLC State parameter is configurable when you click on the Apply button on the VLAN Service (Create) form.

5 Click on the VLAN tab.

6 Set the Application parameter to L2-VPN (TLS/VLAN-Stacking).

7 Click on the Select button in the Group panel to choose a group to associate with the L2 VPN. The Select Group - VLAN Service form opens.

8 Select a group and click on the OK button. The Select Group - VLAN Service form closes and the VLAN (Create) form reappears with the group information displayed.

9 On the navigation tree, right-click on VLAN and choose Create VLAN Site. The Select Network Elements - VLAN form opens.

10 Select a site and click on the OK button. The Select Network Elements - VLAN form closes and the Site (Create) form opens with the site information displayed in the General tab.

11 Configure the parameters.

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State

12 Click on the Select button to choose a customer to associate with the VLAN. The Select Customer - VLAN Service form opens.

13 On the navigation tree, right-click on Ethernet Services and choose Create Ethernet Service. The Ethernet Service (Create) form opens with the General tab displayed.

14 Configure the Ethernet Service Name parameter.

15 On the navigation tree, right-click on Ethernet Service and choose Create Service Access Multipoint. The Service Access MultiPoint (Create) form opens with the General tab displayed

16 Configure the parameters:

- Auto-Assign ID
- Service Access Multi-Point ID

17 If you need to apply a SAP policy other than the default one, click on the Clear button to clear the default SAP policy from the SAP Profile panel. Otherwise, go to step 20.

18 Click on the Select button to choose a SAP profile to associate with the service access multipoint. The Select SAP Profile - Service Access MultiPoint form opens.

19 Choose a SAP profile and click on the OK button. The Select SAP Profile - Service Access MultiPoint form closes and the Service Access Multipoint (Create) form reappears with the selected SAP profile information displayed.

20 On the navigation tree, right-click on Service Access Points and choose Create VLAN Service Access Point. The VLAN Service Access Point (Create) form opens with the General tab displayed.

21 Configure the parameters:

- Name
- Description

22 Click on the Port tab.

23 Click on the Select button to choose a port for the VLAN SAP. The Select Terminating Port - VLAN Service Access Point form opens.



Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

24 Use the configurable filter and Search button to choose a port for the VLAN SAP, and click on the OK button. The Select Terminating Port - VLAN Service Access Point form closes, and the VLAN Service Access Point (Create) form displays the port information.

25 Click on the Apply button if you need to add another VLAN SAP. A dialog box appears. Otherwise go to step 29.

26 Click on the OK button. The VLAN SAP appears in the list of service access points in the service navigation tree.

27 Click on the General tab.

28 Repeat steps 21 to 26 to add an additional VLAN service access point.

29 Click on the OK button. The VLAN Service Access Point (Create) form closes and a dialog box appears.

30 Click on the OK button. The Service Access MultiPoint (Create) form reappears.

31 Click on the Customer VLANs tab.

32 Click on the Create button to add a customer VLAN to the service access multipoint. The Customer VLAN (Create) form opens.

33 Configure the parameters:

- Customer VLAN ID
- Map Type

34 Click on the Apply button if you need to add another customer VLAN. A dialog box appears. Otherwise, go to step 37.

35 Click on the OK button.

36 Repeat steps 33 to 35 to add another customer VLAN.

37 Click on the OK button. The Customer VLAN (Create) form closes, and a dialog box appears.

38 Click on the OK button. The Service Access Multipoint (Create) form reappears with the customer VLAN information displayed.

39 Click on the OK button. The Service Access Multipoint (Create) form closes and a dialog box appears.

40 Click on the OK button. The Ethernet Service (Create) form reappears.

41 Repeat steps 15 to 40 to add another service access multipoint to the Ethernet service.

42 Click on the OK button. The Ethernet Service (Create) form closes and a dialog box appears.

43 Click on the OK button. The Site (Create) form reappears.

44 Repeat steps 13 to 43 to add another Ethernet service to the site.

45 Click on the STP tab.

46 Configure the parameters:

- Enable STP
- Enable Flat STP
- Enable 1x1 STP

47 Click on the DHCP Snooping tab if you need to enable DHCP snooping on the VLAN. The DHCP Snooping General tab appears.

48 Click on the Create button. The VLAN Level DHCP Snooping (Create) form opens.

49 Configure the parameters:

- VLAN Level Option-82 Data Insertion
- VLAN Level MAC Address Verification

These parameters are automatically enabled when DHCP snooping is enabled on a VLAN.

50 Click on the OK button. The VLAN Level DHCP Snooping (Create) form closes, and a dialog box appears.

51 Click on the OK button. The DHCP Snooping General tab reappears.

52 Click on the Binding Database tab if you need to add a static entry to the DHCP binding table.

53 Click on the Create button. The DHCP Snooping Binding Database (Create) form opens.

54 Configure the MAC Address parameter.

55 Click on the Select button to choose a port. The Select Port - DHCP Snooping Binding Database form opens.

56 Choose a port from the list and click on the OK button.

57 The DHCP Snooping Binding Database (Create) form reappears.

58 Configure the parameters:

- IP Address
- Lease Time

59 Click Apply to add the static entry to the table. A dialog box appears.

60 Click on the OK button.

61 Repeat steps 52 to 60 for each static entry that you need to add to the binding table.

62 Click the Cancel button to close the DHCP Snooping Binding Database (Create) form.

63 Click on the OK button. A dialog box appears.

64 Click on the OK button. The VLAN (Create) form reappears.

65 Click on the OK button to close the VLAN (Create) form.

Procedure 66-3 To create an OmniSwitch BTV VLAN service

1 Choose Create→Service→VLAN from the 5620 SAM main menu. The VLAN (Create) Service form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the VLAN. The Select Customer - VLAN Service form opens.

3 Choose a customer for the VLAN and click on the OK button. The Select Customer - VLAN Service form closes and the VLAN Service (Create) form reappears with the customer information.

4 Configure the parameters:

- Service ID
- Auto-Assign ID
- SVC Mgr Service ID
- Service Name
- Description
- Service Tier
- Service Priority
- Administrative State
- Current OLC State
- Revert OLC State

The Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.

The SVC Mgr Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.

The Current OLC State parameter is configurable when you click on the Apply button on the VLAN Service (Create) form.

5 Click on the VLAN tab.

6 Set the Application parameter to Broadcast TV (MVR/IPMV).

7 Click on the Select button in the Group panel to choose a group to associate with the VLAN. The Select Group - VLAN Service form opens.

8 Choose a group and click on the OK button. The Select Group - VLAN Service form closes and the VLAN (Create) form opens with the group information displayed.

9 In the IPMVLAN panel, configure the Type parameter.

10 On the navigation tree, right-click on VLAN and choose Create VLAN Site. The Select Network Elements - VLAN form opens.

11 Choose a site and click on the OK button. The Select Network Elements - VLAN form closes and the Site (Create) form opens with the site information displayed in the General tab displayed.

12 Configure the parameters.

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State

13 On the navigation tree, right-click on L2 Access Interfaces and choose Create VLAN Access Interface. The VLAN Access Interface (Create) form opens with the General tab displayed. The VLAN access interface serves as a receiver port on the IP multicast VLAN.

14 Configure the Description parameter.

15 Click on the Port tab.

16 Click on the Select button to choose a port for the VLAN access interface. The Select Terminating Port - VLAN Access Interface form opens.



Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

17 Use the configurable filter and Search button to choose a port for the VLAN access interface, and click on the OK button. The Select Terminating Port - VLAN Access Interface form closes, and the VLAN Access Interface (Create) form displays the port information.



Note — To configure an access interface, a L2 VPN TLS VLAN user port must be created. See Procedure 66-2.

18 Click on the VLAN tab.

19 Configure the VLAN Tagging parameter.

20 Click on the Apply button if you need to add another VLAN access interface and the VLAN access interface appears in the list of access interfaces in the navigation tree. A dialog box appears. Otherwise, go to step 24.

21 Click on the OK button.

22 Click on the General tab.

23 Repeat steps 14 to 21 for each additional VLAN access interface to be added to the site.

24 Click on the OK button. A dialog box appears.

25 Click on the OK button. The VLAN Access Interface (Create) form closes.

26 Right-click on Ethernet Services and choose Create Ethernet Service. The Ethernet Service (Create) form opens with the General tab displayed.

27 Configure the Ethernet Service Name parameter.

28 On the navigation tree, right-click on Ethernet Service and choose Create Service Access MultiPoint. The Service Access MultiPoint (Create) form opens with the General tab displayed.

29 Configure the parameters:

- Auto-Assign ID
- Service Access Multi-Point ID

30 If you need to apply a SAP policy other than the default one, click on the Clear button to clear the default SAP policy from the SAP Profile panel. Otherwise, go to step 33.

31 Click on the Select button to choose a SAP profile to associate with the service access multi-point. The Select SAP Profile - Service Access MultiPoint form opens.

32 Choose a SAP profile and click on the OK button. The Select SAP Profile - Service Access MultiPoint form closes and the Service Access Multipoint (Create) form reappears with the selected SAP profile information displayed.

33 On the navigation tree, right-click on Service Access Points and choose Create VLAN Service Access Point. The VLAN Service Access Point (Create) form opens with the General tab displayed.

34 Configure the parameters:

- Name
- Description

35 Click on the Port tab.

36 Click on the Select button to choose a port for the VLAN SAP. The Select Terminating Port - VLAN Service Access Point form opens.



Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrids. After you do this, the port is listed when you click on the Search button.

37 Use the configurable filter and Search button to choose a port for the VLAN SAP, and click on the OK button. The Select Terminating Port - VLAN Service Access Point form closes, and the VLAN Service Access Point (Create) form displays the port information.

38 Click on the Apply button if you need to add another VLAN SAP. A dialog box appears. Otherwise, go to step 42.

39 Click on the OK button. The VLAN service access point appears in the list of Service Access Points on the service navigation tree.

40 Click on the General tab.

41 Repeat steps 33 to 39 to add an additional VLAN SAP.

42 Click on the OK button. The VLAN Service Access Point (Create) form closes and a dialog box appears.

43 Click on the OK button. The Service Access MultiPoint (Create) form reappears.

44 Click on the Customer VLANs tab.

45 Click on the Create button to add a customer VLAN to the service access multipoint. The Customer VLAN (Create) form opens.

46 Configure the parameters:

- Customer VLAN ID
- Map Type

47 Click on the Apply button if you need to add another customer VLAN. A dialog box appears. Otherwise, go to step 50.

48 Click on the OK button.

49 Repeat steps 46 to 48 to add another customer VLAN.

50 Click on the OK button. The Customer VLAN (Create) form closes, and a dialog box appears.

51 Click on the OK button. The Service Access Multipoint (Create) form reappears with the customer VLAN information displayed.

52 Click on the OK button. The Service Access Multipoint (Create) form closes and a dialog box appears.

53 Click on the OK button. The Ethernet Service (Create) form reappears.

54 Repeat steps 28 to 53 if you need to add another service access multipoint to the Ethernet service.

55 Click on the OK button. The Ethernet Service (Create) form closes and a dialog box appears.

56 Click on the OK button. The Site (Create) form reappears.

57 Repeat steps 26 to 56 if you need to add another Ethernet service to the site.

58 Click on the STP tab.

59 Configure the parameters:

- Enable STP
- Enable Flat STP
- Enable 1x1 STP

60 Click on the DHCP Snooping tab if you need to enable DHCP snooping on the VLAN. The DHCP Snooping General tab appears.

61 Click on the Create button. The VLAN Level DHCP Snooping (Create) form opens.

62 Configure the parameters:

- VLAN Level Option-82 Data Insertion
- VLAN Level MAC Address Verification

These parameters are automatically enabled when DHCP snooping is enabled on a VLAN.

63 Click on the OK button. The VLAN Level DHCP Snooping (Create) form closes, and a dialog box appears.

64 Click on the OK button. The DHCP Snooping General tab reappears.

65 Click on the Binding Database tab if you need to add a static entry to the DHCP binding table.

66 Click on the Create button. The DHCP Snooping Binding Database (Create) form opens.

67 Configure the MAC Address parameter.

68 Click on the Select button to choose a port. The Select Port - DHCP Snooping Binding Database form opens.

69 Choose a port from the list and click on the OK button.

70 The DHCP Snooping Binding Database (Create) form reappears.

71 Configure the parameters:

- IP Address
- Lease Time

72 Click Apply to add the static entry to the table. A dialog box appears.

73 Click on the OK button.

74 Repeat steps 65 to 73 for each static entry that you need to add to the binding table.

75 Click the Cancel button to close the DHCP Snooping Binding Database (Create) form.

76 Click on the Multicast Groups tab.

77 Click on the Create button to add a multicast group address to the site. The Multicast Group (Create) form opens.

78 Configure the Multicast Address parameter.

79 Click on the Apply button if you need to add another multicast address. A dialog box appears. Otherwise, go to step 82.

80 Click on the OK button. The multicast address information appears on the Site (Create) form.

81 Repeat steps 78 to 80 to add another multicast address to the site.

82 Click on the OK button.

83 Click on the Customer VLAN Tags tab.

84 Click on the Create button to add a customer VLAN tag to the site. The Customer VLAN Tag (Create) form opens.

85 Configure the Customer VLAN Tag parameter.

86 Click on the Apply button if you need to add another customer VLAN tag. The customer VLAN tag information appears on the Site (Create) form. A dialog box appears. Otherwise, go to step 89.

87 Click on the OK button.

88 Repeat steps 85 to 87 to add another customer VLAN tag to the site.

89 Click on the OK button.

90 Click on the OK button to the close the Site (Create) form. A dialog box appears.

91 Click on the OK button. The Site (Create) form closes.

92 Click on the OK button to close the VLAN (Create) form.

Procedure 66-4 To create an OmniSwitch VIP VLAN service

1 Choose Create→Service→VLAN from the 5620 SAM main menu. The VLAN (Create) Service form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the VLAN. The Select Customer - VLAN Service form opens.

3 Choose a customer for the VLAN and click on the OK button. The Select Customer - VLAN Service form closes and the VLAN Service (Create) form reappears with the customer information.

4 Configure the parameters:

- Service ID
- Auto-Assign ID
- SVC Mgr Service ID
- Service Name
- Description
- Service Tier
- Service Priority
- Administrative State

The Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.

The SVC Mgr Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.

5 Click on the VLAN tab.

6 Set the Application parameter to VIP VLAN.

7 Click on the Select button in the Group panel to choose a group to associate with the VLAN. The Select Group - VLAN Service form opens.

8 Choose a group and click on the OK button. The Select Group - VLAN Service form closes and the VLAN (Create) form opens with the group information displayed.

9 On the navigation tree, right-click on VLAN and choose Create VLAN Site. The Select Network Elements - VLAN form opens.

10 Choose a site and click on the OK button. The Select Network Elements - VLAN form closes and the Site (Create) form opens with the site information displayed.

11 Configure the parameters.

- Name
- Description
- Monitor Access Interface Operational State

12 Click on the CFM tab.

13 Configure the parameters.

- Level
- MHF-Creation
- Id-permission

14 Click on the OK button. A dialog box appears.

15 Click on the OK button. The Site (Create) form closes.

16 On the navigation tree, right-click on L2 Access Interfaces and choose Create VLAN Access Interface. The VLAN Access Interface (Create) form opens with the General tab displayed. The VLAN access interface serves as a receiver port on the IP multicast VLAN.

17 Configure the Description parameter.

18 Click on the Port tab.

19 Click on the Select button to choose a port for the VLAN access interface. The Select Terminating Port - VLAN Access Interface form opens.



Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

20 Use the configurable filter and Search button to choose a port for the VLAN access interface, and click on the OK button. The Select Terminating Port - VLAN Access Interface form closes, and the VLAN Access Interface (Create) form displays the port information.



Note — To configure an access interface, a L2 VPN TLS VLAN user port must be created. See Procedure 66-2.

21 Click on the VLAN tab.

22 Configure the VLAN Tagging parameter.

23 Click on the Apply button if you need to add another VLAN access interface. The VLAN access interface appears in the list of access interfaces in the navigation tree. A dialog box appears. Otherwise, go to step 27.

24 Click on the OK button.

25 Click on the General tab.

26 Repeat steps 17 to 23 for each additional VLAN access interface to be added to the site.

27 Click on the OK button. A dialog box appears.

28 Click on the OK button. The VLAN Access Interface (Create) form closes.

29 Click on the OK button to close the VLAN (Create) form.

Procedure 66-5 To associate an access interface with a VLAN service

Associate access interfaces (similar to SAPs) with VLAN services, that are the physical ports to which end users connect. Use the L2 Interfaces tab on the VLAN properties form to associate VLAN services with the ports used by end users.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Use the configurable filter and Search button to choose the VLAN service to be associated with an interface, and click on the Properties button. The VLAN - *Service Name* (Edit) form opens.

3 On the navigation tree, click on the site to which you want to associate the new access interface; expand the entries for that site.

4 Right-click on L2 Access Interfaces and choose Create VLAN Access Interface. The VLAN Access Interface (Create) form opens with the General tab displayed.

5 Configure the parameters.

- Description
- Administrative State

6 Click on the Port tab.

7 Click on the Select button to choose a port for the VLAN access interface. The Select Terminating Port - VLAN Access Interface form opens.



Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

8 Use the configurable filter and Search button to choose a port for the VLAN access interface, and click on the OK button. The Select Terminating Port - VLAN Access Interface form closes, and the VLAN Access Interface (Create) form displays the port information.

9 Configure the remaining parameters, if required.

10 Click on the OK button. The VLAN Access Interface (Create) form closes, and a dialog box appears.

11 Click on the OK button. The VLAN - *Service Name* (Edit) form reappears with the new interface displayed in the service navigation tree under Access Interfaces for the site specified in step 3.

12 Click on the OK button. A dialog box appears.

13 Click on the Yes button to confirm the action and close the dialog box. The Manage Services form reappears.

14 Click on the Close button to close the Manage Services form.

Procedure 66-6 To create a VLAN group

1 Choose Manage→VLAN→VLAN Groups from the 5620 SAM main menu. The Manage VLAN Groups form opens.

2 Click on the Create button. The VLAN Group (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Group Name
- Description
- Node Type
- Technology
- Topology
- VLAN Space Management by SAM
- Head Ends

You can configure the VLAN Space Management by SAM parameter when the Node Type parameter is set to 9500.

You can configure the Head Ends parameter when the Node Type parameter is set to OMNI.

4 Click on the Apply button.

5 Click on the Group Members tab.

6 Click on the Create button. The Select Network Elements form opens and a list of available NEs appears. Only NE types specified by the Node Type parameter are displayed in the list.

7 Choose one or more NEs from the list and click on the OK button. A dialog box appears.

8 Click on the OK button. The selected NEs are listed on the VLAN Group (Edit) form.

9 If you enabled the Head Ends parameter, you can add head end NEs to the group. Otherwise, go to step 13.

10 Click on the Add Headend Node button. The Select Network Elements form opens and a list of available NEs appears. Only 7750 SR, 7710 SR, and 7450 ESS NE types are displayed in the list.

11 Choose one or more NEs from the list and click on the OK button. A dialog box appears.

12 Click on the OK button. The selected NEs are listed on the VLAN Group (Edit) form.

13 If you need to apply a span of control to a group, other than the default, click on the Spans tab. Otherwise, go to step 14.

- **i** Click on the Create button. The Select Span(s) - VLAN Group form opens with a list of available spans.
- **ii** Choose one or more spans of control to apply to the VLAN group.
- **iii** Click on the OK button. The Select Span(s) - VLAN Group form closes and a dialog box appears.
- **iv** Click on the OK button.

14 Click on the OK button. A dialog box appears.

15 Click on the Yes button. The VLAN Group (Edit) form closes.

16 A list of VLAN groups appears in the Manage VLAN Groups form.

17 Close the Manage VLAN Groups form.

Procedure 66-7 To delete a VLAN group or group member



Note 1 — You must delete all of the members from a group before you can delete the group.

Note 2 — A 9500 MPR group member cannot be deleted if it is part of a VLAN path.

1 Choose Manage→ VLAN→VLAN Group from the 5620 SAM main menu. The Manage VLAN Groups form opens.

2 Apply a filter, or create and apply a filter, and click on the Search button. A list of VLAN groups appears.

3 Choose a VLAN group from the list.

4 Click on the Properties button. The VLAN Group (Edit) form opens with the General tab displayed.

5 Click on the Group Members tab.

6 If the group does not contain any members, go to step 9. Otherwise go to step 7.

7 Choose one or more members of the VLAN group and click on the Delete button. A dialog box appears.

8 Click on the OK button to delete the group members.

9 Close the VLAN Group (Edit) form. The Manage VLAN Groups form appears.

10 Choose the VLAN group that you need to delete from the displayed list.

11 Click on the Delete button. A dialog box appears.

12 Click on the Yes button to delete the VLAN group.

13 Close the Manage VLAN Groups form.

Procedure 66-8 To add a MEP to an OmniSwitch VLAN service access interface

Perform the procedure to manually add a MEP to an OmniSwitch VLAN service access interface. See Chapter 78 for more information on MEPs.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Use the configurable filter and Search button to choose the VLAN service and click on the Properties button. The VLAN - *Service Name* (Edit) form opens.

3 On the navigation tree, click on the site to which you want to add the MEP; expand the entries for that site.

4 Right-click on the access interface and click on Properties. The VLAN Access Interface (Edit) form opens with the General tab displayed.

5 Click on the MEPs tab.

6 Click on the Create button.

7 Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

8 Select an entry and click on the OK button. The Select Maintenance Entity Group form closes.

9 Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect

10 Click on the OK button. The VLAN Access Interface (Edit) form reappears.

11 Click on the Refresh button to update the MEP list.

12 Repeat steps 6 to 11 to add additional MEPs.

13 Close the VLAN Access Interface (Edit) form to return to the VLAN Service (Edit) form.

14 Close the VLAN Service (Edit) form.

15 Close the Manage Services form.

Procedure 66-9 To configure IGMP on an OmniSwitch VLAN site

OmniSwitch IGMP parameters can be configured globally and per VLAN site. You can configure VLAN site IGMP parameters only after you create the VLAN. VLAN IGMP configuration settings override global IGMP settings. See Procedure 23-47 for information about configuring global OmniSwitch IGMP parameters.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose an OmniSwitch VLAN service.

4 Click on the Properties button. The VLAN *Service Name* (Edit) form opens with the general properties of the service displayed on the General tab.

5 Click on the Sites tab.

6 Choose a site from the list and click on the Properties button. The Site (Edit) form opens with the General tab displayed.

7 Click on the IGMP tab.

8 Choose an entry from the list and click on the Properties button. The IGMP (Edit) form opens with the General tab displayed.

9 Configure the following parameters, if required:

- Administrative State
- Querying
- Spoofing
- Proxying
- Query Interval (seconds)
- Last Member Query Interval (tenths of seconds)
- Query Response Interval (tenths of seconds)
- Robust Count
- Querier Forwarding
- Zapping
- Max Group Action
- Max Group
- Protocol Version
- Router Timeout (seconds)
- Source Timeout (seconds)
- Unsolicited Report Interval (seconds)



Note — When the Administrative State parameter is Up, IP multicast switching is enabled on the OmniSwitch for standard and L2 VPN (TLS/VLAN-Stacking) VLAN services.

10 Click on the Multicast Group tab to create a static IGMP group.

11 Click on the Create button. The Group (Create) form opens.

12 Click on the Select button to choose a terminating port. The Select Port - Group form opens with a list of available ports.

13 Choose a port from the list and click on the OK button. The Select Port - Group form closes and the selected port appears on the Group (Create) form.

14 Configure the Multicast Group IP Address parameter.

15 Click on the OK button. The Select Port - Group form closes, the multicast group appears in the listing, and a dialog box appears.

16 Click on the OK button.

17 Repeat steps 11 to 16 for each multicast group that you need to add.

18 Click on the Multicast Neighbor tab to create a static IGMP neighbor.

19 Click on the Create button. The Neighbor (Create) form opens.

20 Click on the Select button to choose a terminating port. The Select Port - Neighbor form opens with a list of available ports.

21 Choose a port from the list and click on the OK button. The Select Port - Neighbor form closes and the selected port appears on the Neighbor (Create) form.

22 Click on the OK button. The Select Port - Neighbor form closes, the multicast neighbor appears in the listing, and a dialog box appears.

23 Click on the OK button.

24 Repeat steps 19 to 23 for each multicast neighbor that you need to add.

25 Click on the Multicast Querier tab to create a static IGMP querier.

26 Click on the Create button. The Querier (Create) form opens.

27 Click on the Select button to choose a terminating port. The Select Port - Querier form opens with a list of available ports.

28 Choose a port from the list and click on the OK button. The Select Port - Querier form closes and the selected port appears on the Querier (Create) form.

29 Click on the OK button. The Select Port - Querier form closes, the multicast querier appears in the listing, and a dialog box appears.

30 Click on the OK button.

31 Repeat steps 26 to 30 for each multicast querier that you need to add.

32 Click on the OK button to close the IGMP (Edit) form.

33 Click on the OK button to close the Site (Edit) form

34 Click on the OK button to close the VLAN (Edit) form

35 Click on the Yes button to confirm the action. The VLAN *Service Name* (Edit) form closes and the Manage Services form reappears.

36 Click on the Close button to close the Manage Services form.

Procedure 66-10 To run an OAM validation test on a VLAN service

A validator test suite must be created for the tested entity. See chapter 77 for more information about how to create a validator test suite.



Note — As an alternative, you can also run an OAM validation test on the service by performing a One Time Validation. This is a mostly automated procedure and is described in Procedure 77-9.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a service and click on the Properties button. The VLAN (Edit) form opens with the General tab displayed.

4 Click on the Validate button. If the Validate button is not visible, click on the More Actions button and choose Validate. If a validator test suite is not associated to the service, a dialog box appears. Perform the following steps:

   i Click on the OK button to associate the service with an existing validator test suite. The Choose Validator Test Suite form appears.

   ii Configure the filter criteria. A list of validator test suites appears.

   iii Select a validator test suite and click on the OK button. The Choose Validator Test Suite form closes.

5 View the State Cause indicators. When the validation test fails, a check mark beside the OAM Validation Failure indicator.

6 Click on the Tests tab.

7 Click on the Tested Entity Result tab.

8 Select an entry and click on the Properties button. The Tested Entity Result form opens and displays information about the validation test.

9 Close the Tested Entity Result form.

10 Close the VLAN (Edit) form.

11 Close the Manage Services form.

Procedure 66-11 To view the VLAN service operational status

The Aggregated Operational State and State Cause indicators on the General tab of the service management form display information about service faults.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a service and click on the Properties button. The VLAN (Edit) form opens.

4 View the Aggregated Operational State and State Cause indicators. When the Aggregated Operational State is Down or Partially Down, a check mark beside the appropriate State Cause indicator identifies the type of associated service fault.

5 Click on the appropriate tab to view or edit an object that is identified as faulty by a State Cause indicator.

6 Click on the Faults tab to view the alarms for the object. The Object Alarms tab appears.

7 Click on the Aggregated Alarms tab to view the aggregated alarms for the object. The Aggregated Alarms tab appears.

8 Close the VLAN (Edit) form.

9 Click on the Close button to close the Manage Services form.

Procedure 66-12 To view the service topology associated with a VLAN

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VLAN service and click on the Topology View button. A Topology View dialog box appears.

4 Click on the Yes button to proceed. The Service Topology - *Service Name* map opens.

See chapter 6 for more information about service topology views.

Procedure 66-13 To modify a VLAN service



Caution — Modifying parameters can be service-affecting.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VLAN service.

4 Click on the Properties button. The VLAN *Service Name* (Edit) form opens with the general properties of the service displayed on the General tab.

The following tabs contain non-configurable parameter information for the service:

- VLAN tab—displays information about the VLAN type
- MVR tab—displays multicast package policy information for the service

The MVR tab is not selectable for some types of VLAN.

The following tabs list the service elements that can be individually or collectively selected and configured:

- Sites tab—lists the sites that are included in the service
- VLAN Access Interfaces tab—lists the L2 access interfaces that are included in the service
- Ethernet Services—lists the Ethernet services
- Service Termination Point tab — lists the ports on the far end points of the service
- Template tab — displays the template used to create the mirror service, if applicable.
- Faults tab—displays the faults associated with the service

The Ethernet Services tab is not selectable for some types of VLAN.



Note — Users with the administrator scope of command role can click on the Select button on the Templates tab to associate a service template with the service object, if required.

5 Modify the parameters for the service as required.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button to confirm the action. The VLAN *Service Name* (Edit) form closes and the Manage Services form reappears.

8 Click on the Close button to close the Manage Services form.

Procedure 66-14 To delete a VLAN service



Warning — Deleting a service may result in a service disruption for customers. Consider the implication of deleting the service before proceeding.



Caution — Do not delete any VLANs that are used for network management, otherwise connectivity between the 5620 SAM and the OmniSwitch devices is lost.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 As required, configure the filter criteria to locate the service or range of services to be deleted. A list of services appears at the bottom of the Manage Services form.

3 Choose a service or a range of services from the list.

4 Click on the Delete button. A warning form appears. This message is dynamic based on the priority of the service. Perform one of the following:

   a For services with a low priority, go to Step 5.

   b For services with a medium priority, configure the “Enter the highest priority of the service being deleted” text field by typing: Medium. Go to Step 5.

   c For services with a high priority, configure the “Enter the highest priority of the service being deleted” text field by typing: High. Go to step 5.

5 For all services regardless of how their priority is configured, acknowledge the check box that prompts you confirm that you understand the implications of deleting the service.



Note — If you select multiple services with different priorities, you must enter the highest priority level of selected services before you can delete the services.

6 Click on the Yes button to confirm the action. The service is deleted and removed from the list.

7 Click on the Close button to close the Manage Services form.

67 — VLL service management

67.1 VLL service management overview *67-2*

67.2 Sample VLL service *67-19*

67.3 Workflow to create a VLL service *67-21*

67.4 VLL service management procedures *67-23*

67.1 VLL service management overview

The 5620 SAM supports the provisioning of VLL services on edge devices. A VLL service is an L2 point-to-point service that connects access interfaces. A VLL service is completely transparent to customer or subscriber data and to control protocols. Because of this, the device performs no MAC learning in a VLL service.

The 5620 SAM supports multiple variations of VLL services. See "VLL types" in this section for more information.

A VLL service that connects access interfaces on one device is called a local VLL service. As there is no need for signaling between devices, a local VLL service uses no SDPs.

A VLL service that connects access interfaces on two devices is called a distributed VLL service. Subscriber or customer data enters a distributed VLL service through access interfaces on different edge devices. The VLL service encapsulates the data and transports it across a service provider IP/MPLS network through GRE or MPLS service tunnels.

Packets that arrive at an edge device are associated with a VLL service based on the access interface on which they arrive. An access interface is uniquely identified using these parameters:

- physical port or POS port and channel
- encapsulation type
- encapsulation identifier (if required, depending on encapsulation type)

A VLL service uses T-LDP signaling, and uses MPLS or GRE as the service tunnel transport.

A new or existing VLL can be configured as the spoke of an HVPLS. See "HVPLS" in section 68.1 and chapter 74 for more information.

The 5620 SAM supports end-to-end VLL configuration using the following methods:

- Tabbed configuration forms with an embedded navigation tree. The navigation tree provides a logical view of the service and acts as a configuration interface.
- Preconfigured template. A user who is assigned the template management role can create a service template. The template management user can also configure and bind site, circuit, and L2 interface templates to the service template. See the *5620 SAM Scripts and Templates Developer Guide* for more information about the administrative tasks associated with service templates.

Common to all device services, such as VLL, are policies that are assigned to the service. Policies are defined at a global level and can then be applied to components of the service, such as interfaces or circuits, when the service is configured or modified. The following policies are common to all device services:

- QoS policies define ingress classification, policing, shaping, and marking on the ingress side of the interface. QoS policies are configured using the Access Ingress Policy form, the Access Egress Policy form, and the ATM QoS Policy form. Because a VLL service is a point-to-point service, ingress QoS policies create only the unicast queues that are defined in the policy and not the multicast queues.
- (Epipe service only) Policer control policies to control access ingress policers and access egress policers under a common hierarchy. Policer control policies are configured using the Policer Control Policy Manager.
- Scheduling policies define hierarchical rate limiting and scheduling to govern the scheduling of queues. Scheduler policies are configured using the Scheduler Policy and HSMDA Scheduler Policy forms.
- Port scheduler policies define hierarchical bandwidth allocation and scheduling at the egress port level. Port scheduler policies are configured using the Port Scheduler Policy form.
- Filter policies control network traffic into or out of an interface or circuit based on IP or MAC matching criteria. Filter policies are configured using the ACL IP Filter form and the ACL MAC Filter form.
- Accounting policies measure the traffic on a service to ensure proper billing and enforcement of SLAs. Accounting policies are configured using the Accounting Policy form.
- ANCP policies provide status and control information based on port-up and port-down messages and changes to the current access line rate between the edge device and the access node. ANCP policies are configured using the Manage Subscriber Policies form.
- Time of day suites specify time and day restriction policies that are assigned to QoS policies and schedulers, ACL filters, and aggregation schedulers. Time of day suites and time range policies are configured using the Time of Day Suite form and Time Range form, respectively.

See chapter 42 for more information about policies.

OAM diagnostics can be performed on a per-service basis. See chapter 32 for more information.

The General tab of the VLL service management form displays information about the operational state of the service and its sites through the Operational State and State Cause indicators.

The Operational State indicator identifies the states of the sites that are part of the service, as follows:

- Up—one operational path in both directions (end-to-end)
- Down—path is not operationally complete

When the Operational State is Down, a check mark appears beside the appropriate State Cause indicator to identify the type of fault to the 5620 SAM operator.

You can run the OAM Validation test suite for the service by clicking on the Validate button. If the Validate button is not visible, click on the More Actions button and choose Validate. Alternatively, you can also perform a One Time Validation. If a check mark appears beside the OAM Validation Failed state cause indicator, the test has failed. In addition, the Tested Entity Result tab on the Tests tab displays detailed information about the OAM test result. See chapter 77 for more information about how to configure OAM validation test suites.

The 5620 SAM also monitors the status of a peer SAP after a VLL has been created and put into service. Status information includes faults detected on the service tunnel, and access and network SAP transmissions and receptions. The States tab of the Spoke SDP Binding form displays indicators of failure in the VLL in the State Cause panel.

When you use the 5620 SAM to create or discover a service, the 5620 SAM assigns a default Service Tier value to the service. The Service Tier parameter value is relevant only in the context of composite service topology views. See chapter 74 for more information about the hierarchical organization of composite services.

VLL types

The 5620 SAM supports the creation of the following VLL service types:

- Epipe, or Ethernet VLL service
- Apipe, or ATM VLL service
- Fpipe, or frame relay VLL service
- Hpipe, or HDLC service
- Ipipe, or IP interworking VLL service
- Cpipe, or circuit emulation VLL service

See the *5620 SAM MPR User Guide* for 9500 MPR/9500 MPRe device VLAN service management configuration information.

Epipe (Ethernet VLL)

An Epipe, or Ethernet VLL service, provides a point-to-point Ethernet service. One endpoint of an Epipe uses Ethernet encapsulation, and the other endpoint uses Ethernet, ATM, frame relay, or CEM encapsulation. An Epipe effectively provides ATM and frame relay bridged encapsulation termination for interworking. The 5620 SAM supports local cross-connecting when the Epipe endpoints are on the same device. The device supports these Epipe connectivity scenarios:

- a frame relay or ATM user in an ATM network communicating with an Ethernet user on an IP/MPLS network
- a frame relay or ATM user who connects to a PE device in an IP/MPLS network and communicates with an Ethernet user who connects to another PE device in the same network

ATM users connect through a UNI using AAL-5 or bridged Ethernet PDUs, and use the VCI/VPI as the ATM SAP identifier. Frame relay users connect through a UNI that uses Multiprotocol Interconnect over frame relay or bridged Ethernet PDUs, or over an Ethernet UNI interface. The DLCI is the frame relay SAP identifier. The VCI/VPI and DLCI identifier tags are transparent to the service and remain unaffected during transport.

Devices which support MEF 8 can support TDM services encapsulated on Epipe services using circuit emulation mode. A SAP with a TDM port can then be assigned to an Epipe service using CEM encapsulation. The TDM SAP defines a local and remote ECID as well as a remote MAC address. The MAC address of the TDM port is used as the source MAC address for the emulated circuit.

MEF 8 can be configured on an Epipe service in the following two scenarios:

- one TDM SAP and one Ethernet SAP
- one TDM SAP and one spoke SDP

Using MEF 8 functionality to emulate TDM services, Epipe services can interoperate with devices that support MEF 8 Epipe services, but not MPLS Cpipe services, such as the 9500 MPR. MEF 8 is supported on the 7750 SR, 7450 ESS, and 7710 SR, as well as the 7705 SAR, Release 6.0 R1 or later.

The 5620 SAM supports the following Ethernet SAP encapsulations for an Epipe service:

- null
- dot1q
- QinQ
- SONET/SDH BCP-null
- SONET/SDH BCP-dot1q

Epipe services allow you to designate a dot1q encapsulated SAP as the default SAP for a specific port. For more information about how you can use default SAPs on an Ethernet port, see "Default SAPs" in section 68.1.

A default SAP can co-exist with other SAPs on a port, but it cannot be implemented on a null encapsulated port. You can use the 5620 SAM GUI to create a default SAP by specifying an outer encapsulation value of 4095 or * for a SAP. If OSSI is used, the outer encapsulation value is always 4095.

You can configure a 3-plus-tag Epipe service on the 7210 SAS-M (in network mode) and 7210 SAS-X, Release 5.0 R2 or later. A 3-plus-tag Epipe service enables processing of packets with more than two tags when received on a QinQ SAP. A 3-plus-tag Epipe service requires the configuration of a QinQ SAP as one endpoint and one of the following as the other endpoint:

- a spoke SDP binding
- a dot1q L2 access interface
- a QinQ L2 access interface (supported on NE release 5.0 R3 or later)

The spoke SDP binding must be of VC type VLAN, and the encapsulation values, or tags, must be configured to match. See Procedures 67-2, 67-4, 67-27, and the NE documentation for more information.

Ethernet CFM is supported for 3-plus-tag Epipe services on NE release 5.0 R3 or later.

Apipe (ATM VLL)

An Apipe, or ATM VLL service, provides a point-to-point ATM service between users who connect to 7750 SR, 7710 SR, 7705 SAR, 7950 XRS, or 7450 ESS NEs in an IP/MPLS network directly or through an ATM access network. One endpoint of an Apipe uses ATM encapsulation and the other endpoint uses ATM or frame relay encapsulation. An ATM PVC—for example, a VC or a VP—is configured on the managed device. As a result, the ATM switches at the service endpoints appear to be directly connected over an ATM link. The 5620 SAM supports VPI/VCI translation in an Apipe and supports local cross-connecting when the Apipe endpoints are on the same managed device.

An Apipe encapsulates standard UNI/NNI cells that ingress the ATM SAP into a pseudowire packet using N:1 cell mode encapsulation or AAL-5 SDU mode encapsulation. When using N:1 cell mode encapsulation, an Apipe supports cell concatenation into a pseudowire packet and the setup of both VC- and VP-level connections.

For ATM and frame relay interworking, an Apipe provides a point-to-point service between a user who connects to an existing ATM network and another user who connects to a PE in an IP/MPLS network. An ATM AAL-5 SDU pseudowire or a frame relay 1-to-1 mode pseudowire connects the nodes. The PE performs an FRF.5 interworking function to join the ingress and egress data paths.

An ATM VT SAP on a PE is identified by the physical port and VPI range. Cells that arrive on a specified port and are within the specified VPI range go into a single pseudowire for transport through the IP/MPLS network. A user can configure the whole ATM port as a VT and does not need to specify a VPI range. There is no ingress or egress VPI/VCI translation or loss of cell order.

The 7705 SAR uses N>1 cell mode encapsulation to support multiple VCs on an Apipe. You can multiplex VCs on a 7705 SAR Apipe service using SAP aggregation groups. See Procedure 67-43 for more information about how to configure SAP aggregation groups.

The 5620 SAM supports the ATM N:1-N>1 VC type to allow interoperability between 7705 SAR and 7750 SR Apipe services, despite each site using different cell mode encapsulation. An interoperating Apipe service uses the ATM N:1-N>1 VC type, while the 7705 SAR site uses ATM VCC and the 7750 SR uses ATM Cell. An interoperating Apipe service combines SAP aggregation groups from the 7705 SAR Apipe with connection profiles from the 7750 SR Apipe onto a single Apipe service. See chapter 53 for more information about connection profiles.

Fpipe (frame relay VLL)

An Fpipe, or frame relay VLL service, provides a point-to-point frame relay service between users who connect to PE 7750 SR, 7710 SR, or 7450 ESS NEs in an IP/MPLS network. Both endpoints of an Fpipe use frame relay encapsulation. An Fpipe connects users through frame relay PVCs. An Fpipe receives standard Q.922 core frames on the frame relay SAP and encapsulates them in a pseudowire packet according to the 1-to-1 frame relay encapsulation mode. This is the VC type used on the SDP by default. The 5620 SAM does not support the many-to-one, or port encapsulation, mode. Fpipe creation supports local cross-connecting when the endpoints are on the same managed device.

Hpipe (HDLC VLL)

An Hpipe, or HDLC VLL service, is used to carry HDLC PDUs over an MPLS network. HDLC PWs enable service providers to offer emulated HDLC services over existing MPLS networks. HDLC mode provides port-to-port transport of HDLC-encapsulated traffic.The HDLC PDU is transported in its entirety, including the HDLC address and control fields, but the HDLC flags and the FCS are excluded. If the optional control word is used, the flag bits in the control word are not used and must be set to 0 for transmitting and must be ignored upon receipt.

Before HDLC SAPs can be configured, the mda-mode command must be set to cem-fr-hdlc-ppp at the card level. Only ports that are configured with HDLC encapsulation can be mapped to an Hpipe SAP.HDLC encapsulating ports do not terminate the HDLC. The ports pass the HDLC frames through the Hpipe. HDLC encapsulated ports can pass through any HDLC-framed traffic, such as Cisco-HDLC, FR, PPP, etc.

Ipipe (IP interworking VLL)

An Ipipe, or IP interworking VLL service, uses the IP/MPLS network to provide Layer 3 connectivity between different Layer 2 technologies. An Ipipe service provides point-to-point IP connectivity between a user on a frame relay, ATM, cHDLC, or PPP access circuit with routed PDU IPv4 encapsulation and a user on an Ethernet interface. The Ethernet SAP interface can terminate on a 7705 SAR, 7750 SR, 7450 ESS, 7710 SR, or 7950 XRS.

Table 67-1 summarizes the supported SAP types.

Table 67-1 Supported SAP types

SAP Types	Frame relay	ATM	PPP/IPCP	cHDLC	Ethernet
Frame relay	✓	✓			✓
ATM	✓	✓			✓
PPP/IPCP			✓		✓
cHDLC				✓	✓
Ethernet	✓	✓	✓	✓	✓

In an Ipipe service, both CE devices appear to be on the same IP interface. The PE devices must therefore resolve Layer 2 addresses when different resolution protocols are used on either SAP. Each PE device is manually configured with the IP addresses of both CE devices, or alternatively, can be set to automatically discover the IP addresses of the CE routers. The PE device maintains an ARP cache context for each IP interworking VLL, and responds to ARP request messages received on the Ethernet SAP. The PE device responds with the Ethernet SAP configured MAC address as a proxy for an ARP request for the frame relay, ATM, or PPP user access circuit IP address, and silently discards any ARP request message received on the Ethernet SAP for any other address. The PE device maintains a record of the association of IP addresses with MAC addresses for ARP requests that it receives over the Ethernet SAP.

An Ipipe SAP can be bound to a physical or logical port with PPP, cHDLC, ATM, or FR encapsulation. On Release 8.0 R5 or earlier NEs, when IPv6 is enabled, cHDLC, ATM and FR encapsulation are not supported. ATM users connect through a UNI using AAL-5 MUX IP or AAL-5 SNAP routed PDU encapsulation. Frame relay users connect using routed PDU IPv4 encapsulation. PPP interfaces use PPP/IPCP encapsulation of an IPv4 packet. Users of cHDLC connect using routed IPv4 encapsulation.

The 5620 SAM supports the following Ethernet SAP encapsulations for an Ipipe service:

- Null
- dot1q
- QinQ



Note — IPCP SAPs on the 7705 SAR can be configured to assign primary and secondary DNS addresses to the remote peer.

The following identifiers are used for packet forwarding:

- VCI/VPI as the ATM SAP identifier
- DLCI as the frame relay SAP identifier

Cpipe (circuit emulation VLL)

A Cpipe, or circuit emulation VLL service, provides a point-to-point CEM service between users who connect directly to 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, 7705 SAR, 7710 SR, or 7750 SR devices, or to 7450 ESS devices in an IP/MPLS network. The endpoints of a Cpipe use CEM encapsulation.



Note — The creation of point-to-point Cpipe CEM services on a 7450 ESS is supported only on a 7450 ESS, Release 8.0 R5 or later.

The Cpipe L2 access interface can be bound to a unstructured DS1 or E1 channel, a channelized DS0 channel group, or a DS0 group with CAS signalling. Consider the following when creating a Cpipe:

- The Time Slots parameter of the DS0 channel must be configured with at least one time slot.
- Time slots are automatically configured for unstructured E1 and T1 endpoints.
- The Clock Source parameter of the DS1 channel must be set to Node-Timed.

VLL spoke switching

VLL spoke switching allows you to create a VLL service by cross-connecting two spoke SDPs. Spoke switching allows you to scale L2 services, such as VLLs and H-VPLS, over a multi-area network without the requirement for a full mesh T-LDP. The 5620 SAM supports spoke switching on all VLL types, however, all service instances must be the same type.

The 5620 SAM supports VLL services with spoke switching on the 7750 SR, 7450 ESS, and 7950 XRS.

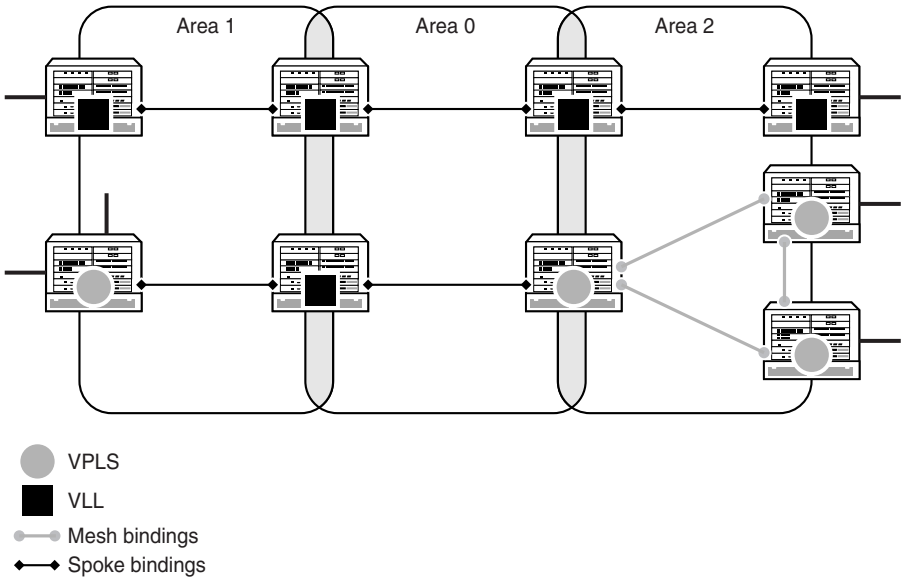
Table 67-2 describes the VLL site types that you can use in a spoke switching configuration.

Table 67-2 VLL site types

VLL site type	Description
Terminating	VLL instance has one or two VLL SAPs.
Switching	VLL instance cross-connects two spoke bindings.

Figure 67-1 shows a switching VLL that connects two VPLS. The configuration uses two T-PEs, three S-PEs, and two pairs of spoke bindings to connect the two VPLS.

Figure 67-1 VLL spoke switching



Configuration requirements

You must consider the following configuration rules when provisioning VLL services with spoke switching:

- Service type must be a VLL at the switching node.
- VC IDs can be different for the segments in the service.
- Segments in the service can run on different types of tunnels; for example, LDP, GRE, and RSVP SDPs.
- VLL instances in a service must use the same service ID to avoid the discovery of multiple and composite services.
- VLL with one or more switching sites must have two or more terminating sites.
- Autobinding creation service is not supported for switching VLLs.

VLL redundancy

VLL redundancy requires that you associate the SAP or SDP bindings to an endpoint. You can configure the endpoint association as active or standby so that you can create a redundant configuration. The associated nodes use signaling to determine the active SAP or SDP binding. The 5620 SAM supports VLL redundancy on the 7450 ESS, 7705 SAR, 7710 SR, 7750 SR, and 7950 XRS.

A VLL service site can have up to two local endpoints. A local endpoint combines a SAP with a binding (access) or a group of bindings (network). A SAP or an SDP binding can also exist without an endpoint association.

The 7450 ESS, 7710 SR, 7750 SR, and 7950 XRS support HSDPA offload fallback for VLL Apipe and Epipe services by allowing fallback from an active PW on a primary spoke SDP to a secondary SAP.

Table 67-3 describes the components in redundant VLL configurations.

Table 67-3 VLL components for redundant configurations

VLL component	Description
Primary or Redundant binding	Primary or redundant binding is the same as a regular spoke binding. Up to four spoke bindings can form a VLL instance network endpoint. Only one binding can be configured as the primary; up to 3 others can only be configured as redundant spokes. Each redundant spoke has a precedence value to decide which spoke is the immediate backup. Only the terminating VLL instance can have multiple bindings on the network side endpoint. A switching VLL instance has up to 2 bindings, one on each side.
Inter-Chassis Backup	You can use an ICB in conjunction with a redundant SAP to provide protection for the SAP. The SAP must also be associated with a MC-LAG or MC-APS port. The ICB transports network traffic to the SAP on the second PE when the local SAP is unavailable. You must define a switching state for the redundant SAP. You must also configure the return ICB on the opposite endpoint of the protected site.

Configuration options

Table 67-4 describes the redundancy configuration options for each VLL site.

Table 67-4 VLL redundancy configuration options

Option	Configuration	Description
1	SAP SDP binding	You can create an endpoint without any SAP or SDP.
2	SAP SAP	You can create an endpoint without any SAP or SDP.
3	SDP binding SDP binding	You can configure this option for switching sites only.
4	SAP Endpoint with SDP bindings (maximum of 4 spokes and 1 ICB)	Figure 67-2 shows the configuration of this option on the PE nodes.
5	Endpoint with SAP/ICB SDP binding	Figure 67-3 shows the configuration of this option on Node B.
6	Endpoint with SAP/ICB endpoint with SAP/ICB	Figure 67-4 shows the configuration of this option.
7	Endpoint with SAP/ICB Endpoint with up to 4 SDP bindings	Figure 67-5 shows the configuration of this option.

Figure 67-2 VLL redundancy configuration - option 4

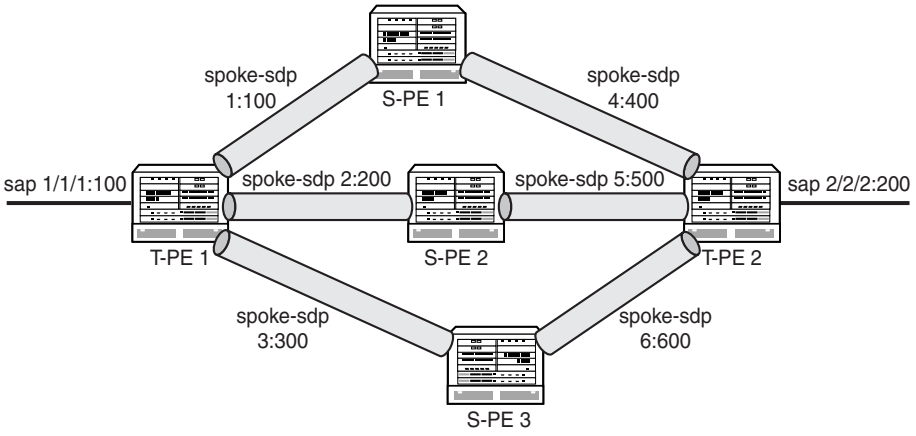


Figure 67-3 VLL redundancy configuration - option 5

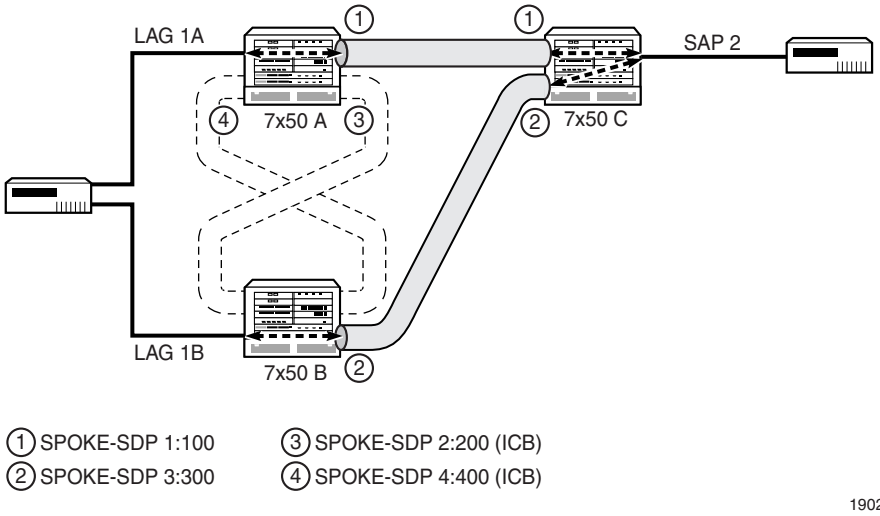
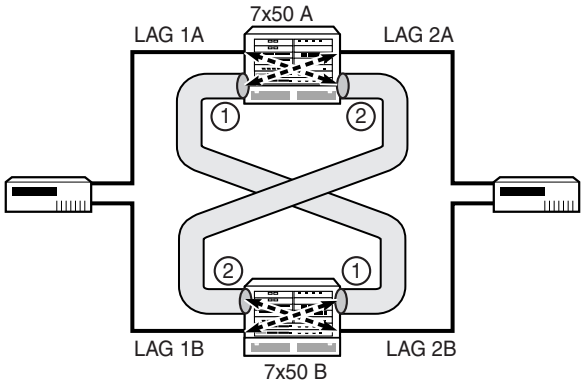


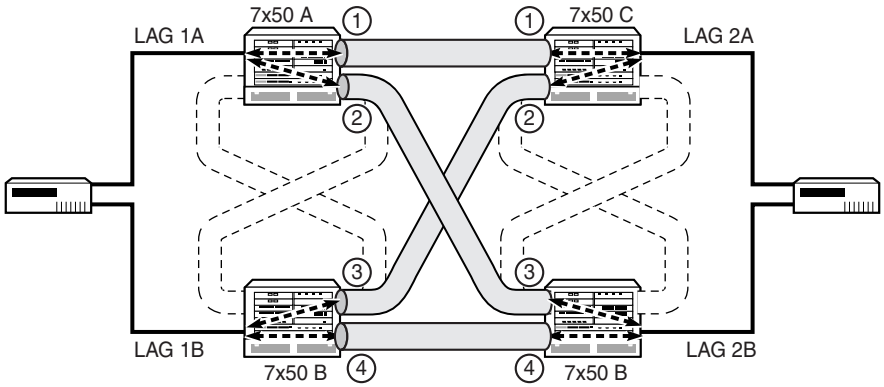
Figure 67-4 VLL redundancy configuration - option 6



1 SPOKE-SDP 1:100 (ICB)
2 SPOKE-SDP 1:200 (ICB)

19023

Figure 67-5 VLL redundancy configuration - option 7



1 SPOKE-SDP 1:100
2 SPOKE-SDP 2:200 (ICB)
3 SPOKE-SDP 3:300 (ICB)
4 SPOKE-SDP 4:400

19024

Configuration requirements

You must consider the following configuration rules when provisioning VLL services with spoke switching and redundancy:

- A VLL service can have one or more VLL instances. An instance can reside on a 7210 SAS-M, 7705 SAR, 7750 SR, 7450 ESS, 7710 SR, or 7950 XRS.
- Local endpoint rules:
  - A VLL instance has a maximum of two endpoints. A terminating VLL instance has at least one access endpoint and a switching VLL instance has two network endpoints.
  - A network endpoint has a maximum of four spoke-bindings, which can include any combination of the following: a single primary spoke, one or more secondary spokes with precedence, and one ICB spoke.
  - A SAP or a binding has a maximum of one endpoint association.
  - An endpoint has a maximum of one SAP.
  - A SAP or a binding with association to an endpoint can be moved to another endpoint or removed from that endpoint.
- SAP rules:
  - A MC-LAG SAP or MC-APS SAP cannot be deleted when there is an ICB on the same endpoint.
  - SAPs cannot exist on switching sites.
  - A maximum of two SAPs can exist for each site.
  - A SAP with a non-ICB spoke cannot exist on the same endpoint.
  - Apipe and Epipe services support MC-APS.
- Spoke binding rules:
  - The SDP types (GRE, MPLS) used by the redundant spoke bindings do not have to be the same when you manually create the spoke bindings.
  - Redundant configurations are not supported for S-PE because there are a maximum of two spoke bindings for a switching VLL instance.
  - An ICB SDP binding should not be created on an endpoint without a MC-LAG SAP or MC-APS SAP.
  - Only one ICB can exist for each endpoint.
  - ICB SDP binding can only have a precedence of 4, the lowest priority.
  - Only one primary spoke can exist for each endpoint.
  - Spoke SDP binding cannot associate with an endpoint on a switching site.
- HSDPA offload fallback rules:
  - Apipe and Epipe services support HSDPA offload fallback on ATM interfaces.
  - The spoke SDP must be configured with primary precedence.
  - The SAP must be configured with MC-APS or ATM channel.
  - When the SAP is configured with MC-APS, the spoke SDP can be configured with ICB.

HSDPA Offload Resiliency

Mobile service providers deliver both voice and data services to their customers using mobile handsets. The data services provided require significantly more bandwidth than voice services. In order to minimize the operational costs (specifically, bandwidth), service providers typically separate the voice and data traffic at the mobile base station. The voice traffic may be backhauled over an ATM infrastructure, while a Metro Ethernet infrastructure (their own or third-party) is used to backhaul the data traffic. The separation of data traffic onto a separate network for backhaul is referred to as High Speed Data-Link Packet Access offload.

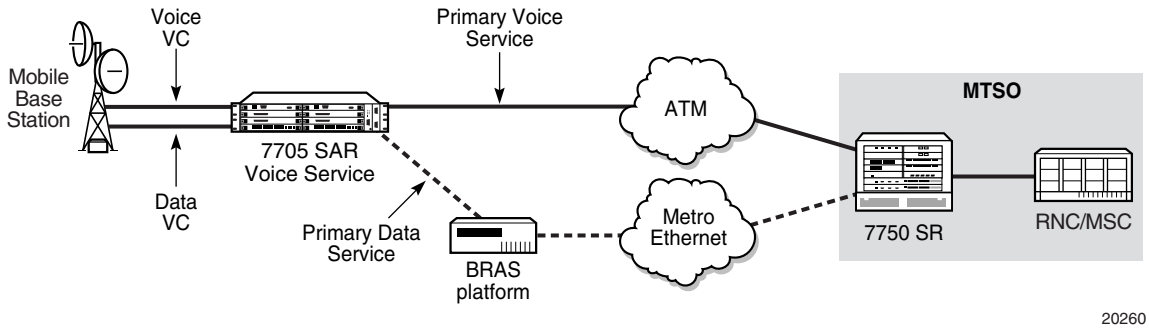
The HSDPA Apipe services traverse a path over the Metro Ethernet network which contains single potential points of failure that are unprotected. The ATM network can be used to provide a transient path for the data service in the event of a failure in the Metro Ethernet infrastructure, as long as the voice traffic is not impacted (data traffic is given lower QoS priority by the 7705 SAR and 7750 SR NEs). Clearly there is potential for the data service to suffer degradation (depending on the bandwidth required), until the fault in the Metro Ethernet network is resolved. However the SLA requirements for the data service are typically best effort.

The ability to switch to this alternate transient pathway for the data service is referred to as HSPDA resiliency.

HSPDA resiliency is implemented through the use of VLL Apipes on the 7705 SAR. The network architecture used in the ATM backhaul scenario is shown in Figure 67-6.

Note — For HSPDA offload resiliency, the primary and secondary services must be on the same NE.

Figure 67-6 ATM-based HSDPA offload architecture - nominal operation



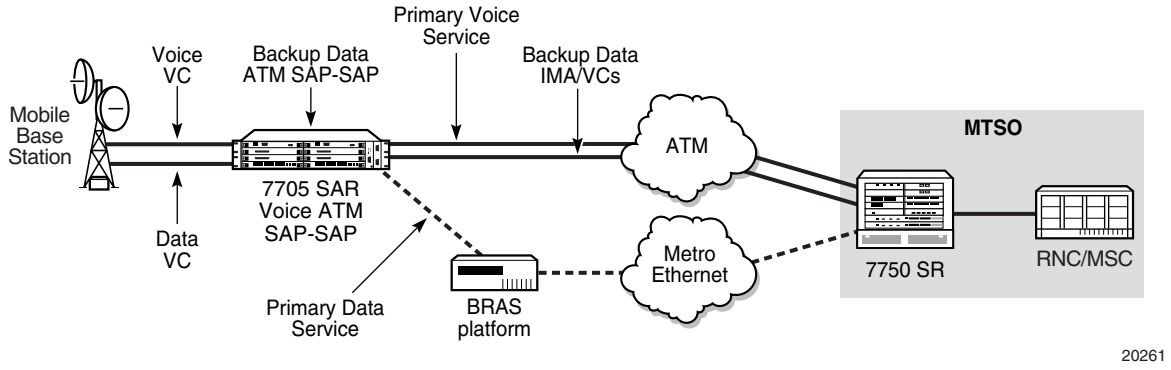
The mobile base station node separates the voice and data traffic and delivers the two different traffic types to the 7705 SAR on different VCs. Both the voice and data services use Apipe pseudo-wires to carry the traffic over the backhaul network to the 7705 SAR. The HSDPA Apipe service is paired with an OAM service (not shown in Figure 67-6) which is used by the wireless infrastructure to monitor the end-to-end path between the wireless endpoints.

For the ATM voice traffic, an internal Apipe is used on the 7705 SAR to switch ATM cells between the access VC/IMA group and the network side VC/IMA group. The service does not span the radio access network between the 7705 SAR and the 7750 SR located at the Mobile Telephone Switching Office (MTSO).

Data Apipe services (HSDPA/OAM) use service tunnels based on either MPLS or GRE. GRE is generally used in the context of a third-party Metro Ethernet network, since there is a Broadband Remote Access Server (BRAS) in the path between the DSLAM and the 7750 SR located at the MTSO (BRAS platforms do not support MPLS). MPLS is typically used when the mobile provider owns the Metro Ethernet network.

When the resiliency solution described below detects a failure in the Metro Ethernet network, its protection mechanism switches the traffic associated with the data service from the path over the Metro Ethernet network to a path which traverses the ATM (shown in Figure 67-7). The detection, switchover, and switchback mechanisms are implemented by the 5620 SAM.

Figure 67-7 HSDPA Offload Protection - ATM data backhaul



A backup (secondary) data service for an active (primary) data service is pre-configured on the 7705 SAR. For a typical 7705 SAR deployment at a cell site, two backup services are required, one for the HSDPA service and one for the OAM service. These backup services are created by the operator during the deployment of the 7705 SAR. A peer resiliency relationship between the active and backup services must also be configured.

The backup services used are internal Apipes. The switchover from primary to secondary is triggered by an event from the 7705 SAR sent to 5620 SAM, which indicates that the service tunnel (SDP) has failed. When the failure event is processed by 5620 SAM, the SAPs on the active data services are moved (along with the associated VCs) from the active service to its peer backup service and are enabled. After the re-configuration of the SAPs on the backup services completes, the traffic is moved to the backup services, which then carry the traffic over the ATM portion of the network. When the switchover is complete, an alarm is raised against the primary service indicating that it has been switched to the secondary service.

Other considerations include the following:

- If a service configured as primary is deleted from 5620 SAM or the CLI, then the corresponding resiliency is also deleted.
- If a service configured as secondary is deleted from 5620 SAM, this is blocked and a pop-up message indicates that the corresponding resiliency must first be deleted.
- If a service configured as secondary is deleted from the CLI, an alarm is raised indicating that the resiliency is misconfigured. If a secondary service is then subsequently added to the resiliency, this alarm is cleared.
- If the SAP initially configured on the primary service is deleted, the 5620 SAM raises an alarm. If the SAP is restored in the same service, the alarm clears.
- When the 5620 SAM detects that a failed SDP is up, which indicates that the primary service has recovered, the resiliency is set to the Secondary (Debounced) state and a damping timer is started. If the SDP goes down while the resiliency is in the Secondary (Debounced) state, the resiliency changes to the Secondary state and the damping timer stops. If the SDP changes state during the damping time, the value of the damping timer doubles until it rises to the maximum damping time. This prevents the service from flapping between primary and secondary. If the SDP does not change operational state during the damping time, the resiliency is set to Primary, the SAP is moved from the secondary to the primary service, and the alarm related to the service switch clears.
- After the primary service is restored, the damping timer value is set back to its initial value. The damping timer value is not displayed. The initial damping time is 30 000 ms; the time doubles, if required, to a maximum of 480 000 ms.
- The availability of this HSDPA resiliency feature is controlled by the 5620 SAM license key. If this feature is enabled using the 5620 SAM license key, then the Manage→Redundancy→HSDPA Resiliency feature is available on the main 5620 SAM menu, otherwise it does not appear. This feature also requires the SAM(P) module. A new package is added to the 5620 SAM License form called the Mobile Services Package. The HSDPA Resiliency feature is available when this package is enabled.

SDP bindings bandwidth allocation

You can administratively account for the bandwidth used by VLL services inside an RSVP SDP that consists of RSVP LSPs. The SR service manager keeps track of the available bandwidth for each SDP.

When you create a service tunnel, you configure an SDP Bandwidth Booking Factor percentage, which is applied to the SDP available bandwidth. You then assign an SDP Admin Bandwidth value (in kbps) to the spoke SDP. When you bind a VLL service to this SDP, this amount of bandwidth is subtracted from the adjusted available SDP bandwidth. If you subsequently delete the VLL service binding from this SDP, this bandwidth amount is added back into the adjusted SDP available bandwidth. If you overbook the total adjusted SDP available bandwidth when adding a VLL service, a warning is issued and the binding is rejected.

This feature does not guarantee bandwidth to a VLL service, as there is no change to the data path to enforce the bandwidth of an SDP by means such as shaping or policing of the constituent RSVP LSPs. Also, this feature does not provide a CAC capability for a local VLL service which consists of a cross-connect between two SAPs.

In addition, if multipoint services such as VPLS and VPRN are using the same SDP for forwarding packets, the amount of bandwidth consumed by these services is also not accounted for. Therefore, it is advisable to dedicate an SDP for VLL services for which bandwidth reservation is required. Furthermore, VPLS and VPRN services which use separate SDPs but which forward packets over the same network port as the VLL SDP also do not have their bandwidth accounted for. This may impact the bandwidth available to the VLL services.

Auto SDP binding (for all spoke bindings or just the return binding) cannot be used when there is a bandwidth request for the binding. The converse also applies. An error message appears when saving the configuration if this conflict occurs. 5620 SAM checking is done for OSSI.

Port redundancy

Cpipe and Epipe services on 7450 ESS, 7705 SAR, 7710 SR, and 7750 SR devices support port redundancy, which allows you to define a backup port or channel for a VLL SAP. The backup port or channel can be on the local site, for what is called on-node switching, or on a remote site, for what is called off-node switching. In the event of a failure on the SAP, you can manually switch to the backup port or channel using a button on the VLL service, site, or SAP properties form, or from the port properties form.

When a SAP is switched to a backup port using off-node switching, the primary SAP on which the switching is performed is deleted along with the site and site child objects, including the associated SDP bindings. The site is subsequently created on the backup NE, as are the SAP and the other site child objects, using the same tunnel type and tunnel profile for SDP bindings as the primary site.

See Procedure 67-27 for configuration information. See Procedures 67-41 and 67-42 for information about switching between the redundant ports of one or multiple VLL SAPs.



Caution — Alcatel-Lucent recommends that you set the OLC state of a service to Maintenance before you switch to a redundant port or channel, and reset it to the previous state after the switch is complete.



Note 1 — Ethernet OAM objects, for example, MEPs, that are associated with the protected SAP are not copied to the new SAP.

Note 2 — When multiple SAPs are selected, switching is attempted only for the SAPs that support port redundancy and on which port redundancy is properly configured.

Note 3 — Port redundancy switching fails if the SAP or port is included in one of the following redundancy objects:

- BGP-MH
- MC-APS
- MC-LAG
- MC-ring

Copying and moving SAPs between ports

You can copy and move SAPs between ports. See section "Moving and copying SAPs between ports" in chapter 16 for more information.

DoS protection

To protect a VLL from a high incoming packet rate that characterizes a DoS attack, you can use the 5620 SAM to create DoS protection policies for VLL Epipe or Ipipe L2 access interfaces. A DoS protection policy limits the number of control-plane packets that an interface receives each second, and optionally logs a violation notification if a policy limit is exceeded. You can use the NE System Security form to view the violations for a specific NE.

You can configure a DoS protection policy to control the following on a VLL Epipe or Ipipe L2 access interface:

- the control-plane packet arrival rate per subscriber host on the interface
- the overall control-plane packet arrival rate for the interface
- whether an NE sends a notification trap if a policy limit is exceeded

Each VPLS L2 access interface on an NE that supports DoS protection is automatically assigned a default DoS protection policy. The default policy limits only the overall packet arrival rate for the interface, and cannot be deleted or modified. See the *5620 SAM System Administrator Guide* for information about creating a DoS protection policy.

DDoS protection

You can configure a DDoS protection policy on a VLL Epipe or Ipipe L2 access interface. See the *5620 SAM System Administrator Guide* for information about configuring a DDoS protection policy.

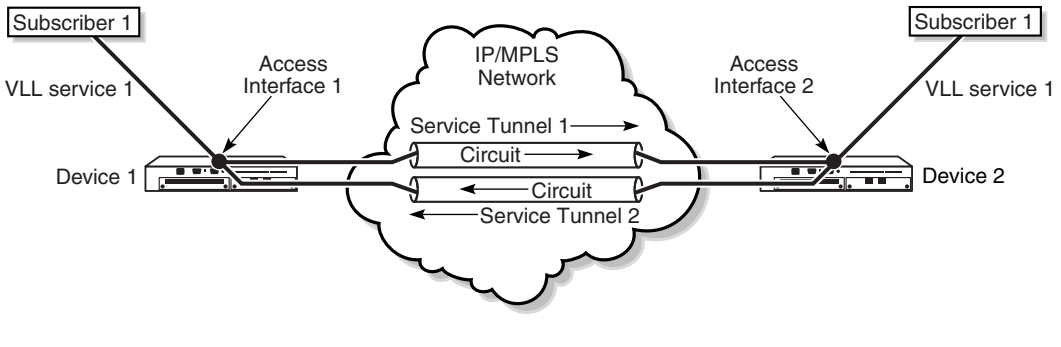
BGP VPWS

You can use the 5620 SAM to create a BGP VPWS, which is an L2 VPN service that uses BGP pseudowire signaling. BGP VPWS is implemented in the 5620 SAM under an Epipe site, which is configured to use BGP to establish a pseudowire with a remote Epipe site. See Procedure 67-54 for information about configuring a BGP VPWS.

67.2 Sample VLL service

Figure 67-8 shows a sample VLL service.

Figure 67-8 Sample VLL service



Assuming the core IP/MPLS network and service tunnels have already been configured, Table 67-5 shows the high-level tasks required to configure this sample VLL service.

Table 67-5 Sample VLL service configuration

Task	Description
1. Configure policies as required	Policies should be configured prior to creating a service. Participation in policies is defined when you configure or modify resources such as access interfaces during VLL service creation or modification. The following key policies can be applied to resources that are part of a VLL service. • Access ingress and egress interface policies. Choose Policies→QoS→SROS QoS→Access Ingress or Access Egress, then the name of the policy you want to configure, to open these forms. • ATM policies. Choose Policies→QoS→SROS QoS→ATM QoS to open the ATM QoS Policies form. • Scheduler policy. Choose Policies→QoS→SROS QoS→Scheduler, then the name of the form you want to configure, to open the scheduler policy forms. • ACL IP and ACL MAC filter policies. Choose Policies→Filter→ACL IP Filter or ACL MAC Filter to open the filter policy form. • Accounting policy. Choose Tools→Statistics→Accounting Policies to open the accounting policy form. • ANCP policy. Choose Policies→Residential Subscriber to open the Residential Subscriber Policies form.
2. Configure ports as access ports for use in the service	If applicable, choose a port from the navigation tree, right-click on the port, and choose Properties from the contextual menu. Specify the port as an access port and specify an encapsulation type, if required.
3. Configure service tunnels as required	Service tunnels are automatically created if there are no tunnels between the source and destination devices. You must choose GRE as the transport type for the 5620 SAM to automatically create service tunnels. To manually create service tunnels, choose Manage→Service Tunnels. Unidirectional service tunnels carry service traffic between edge managed devices using aggregated SDP bindings. SDP bindings can be associated with service tunnels during service configuration. During service creation, you can also configure the 5620 SAM to automatically create and associate service tunnels with SDP bindings. In this case, you do not have to create service tunnels before you create the service. After you have created a VLL, status indicators display selected operational failures on the service tunnel and peer SAP.
4. Create and configure Subscriber 1	Choose Manage→Service→Customers to open the customer manager form and create a customer.

(1 of 2)

Task	Description

5. Create and configure Service 1	Choose Create→Service→VLL→*Type of VLL service*. Use the tabbed form and embedded navigation tree to configure the service. You configure the following key elements when you configure Service 1.
	• Associate Subscriber 1 with the service.
	• Specify Device 1 and Device 2 as the sites for the VLL service.
	• Configure and specify Access Interface 1 and Access Interface 2 as the access interfaces for the VLL service. You do the following when you configure access interfaces.
	  • Specify the ports for the access interfaces. Ethernet ports must be configured as access ports.
	  • Specify participation of the access interfaces in access ingress, access egress, and ATM QoS policies as required.
	  • Specify participation of the access interfaces in aggregation rate limiting across a card or port. If aggregation is not required, specify participation of the access interfaces in ingress and egress scheduler policies. If aggregation is required, specify participation of the access interfaces in an aggregation scheduler policy.
	  • Specify participation of the access interfaces in scheduler policies as required.
	  • Set the ATM OAM Terminate parameter to Up when the VLL L2 access interface port belongs to a MC-APS channel and the VC Type parameter is set to ATM-SDU.
	Create and configure circuits in both directions. Associate the circuit from Device 1 to Device 2 with Service Tunnel 1. Associate the circuit from Device 2 to Device 1 with Service Tunnel 2. You can also configure the 5620 SAM to automatically create and associate service tunnels with circuits.

(2 of 2)

67.3 Workflow to create a VLL service

The following workflow lists the high-level steps required to create a VLL service. As a prerequisite for creating a VLL service, this workflow assumes the following:

- a group or customer with the required user access privileges has been configured.
- the IP or IP/MPLS core network exists.
- any required service tunnels are created including the static or dynamic LSP required to create the service tunnel; see Procedure 27-1.
- the access ports for the service are created; see chapter 16 for more information.
- any required pre-defined routing, QoS, scheduling, filter, accounting, and time of day suite policies are created; see chapter 42 for more information. You do not have to create pre-defined policies if policies are created on a per-service basis.
- any required MP-BGP for PE-to-PE routing is configured; see chapter 23 for more information about protocol configuration.

1 Create and configure the VLL service:

i Define the VLL service type as Epipe, Apipe, Fpipe, Hpipe, Ipipe, or Cpipe.

- For VLL Epipe services; see Procedure 67-1.
- For VLL Apipe services; see Procedure 67-8.
- For VLL Fpipe services, see Procedure 67-12.
- For VLL Hpipe services, see Procedure 67-15.
- For VLL Ipipe services, see Procedure 67-18.
- For VLL Cpipe services; see Procedure 67-21.

ii Specify the NEs (sites) used in the service based on the following topologies:

- Traditional VLL: terminating site only
- Switching VLL: switching site with two or more terminating sites
- Redundant VLL: ICB spoke to MC-LAG (Epipe) or MC-APS (for Apipe and Epipe)

iii Specify the following information for redundant VLL services:

- endpoints
- access interfaces for VLL terminating sites

iv Specify the following information to create a VLL Apipe or Epipe HSDPA offload fallback solution:

- endpoints
- SAP on endpoint one with MC-APS or ATM channel
- spoke SDP with ICB on endpoint one
- spoke SDP with primary precedence on endpoint two
- SAP on endpoint two with MC-APS
- spoke SDP with ICB on endpoint two

v Specify aggregation on a service basis, or across a card or port.

vi Specify QoS, scheduling, accounting, ANCP, MEP association and filter policies.

vii Specify the time of day suite.

2 For VLL services created on an OmniSwitch:

a Create VLAN groups and add members to each group as required. See Procedure 66-6.

b Delete a VLAN group or group member. See Procedure 66-7.

3 Turn up the service.

4 Perform one or more of the following as required.

a Configure a GNE site on a VLL service. See Procedure 67-25.

b Create a VLL L2 access interface on a terminating site. See Procedure 67-27.

c Create a SAP aggregation group for a 7705 SAR Apipe. See Procedure 67-43.

d Create an HSDPA resiliency configuration. See Procedure 67-44.

e Activate and manually operate an HSDPA resiliency configuration. See Procedure 67-45.

f Run an OAM validation test for a VLL service. See Procedure 67-46.

g Configure a BGP VPWS. See Procedure 67-54.

5 As required, view VLL information:

a View the service topology map associated with a VLL service. See Procedure 67-47.

b View the VLL service operational status. See Procedure 67-48.

c View the peer status information associated with the VLL service. See Procedure 67-50.

6 As required, modify a VLL service:

a Using the Manage Services form. See Procedure 67-51.

b Using the topology view. See Procedure 67-52.

7 As required, delete a VLL service. See Procedure 67-53.

67.4 VLL service management procedures

Use the following procedures to perform VLL service creation and management task

Procedure 67-1 To create a VLL Epipe service

1 Choose Create→Service→VLL→Epipe (Ethernet to Ethernet/ATM/FR/CEM) from the 5620 SAM main menu. The Epipe Service (Create) form opens.

2 Click on the Select button to choose a customer to associate with the VLL Epipe service. The Select Customer - Epipe Service form opens.

3 Choose a customer for the VLL service and click on the OK button. The Select Customer - Epipe Service form closes and the Epipe Service (Create) form reappears with the customer information displayed.

4 Configure the parameters:

- Service ID
- Auto-Assign ID
- SVC Mgr Service ID
- Default VC ID
- Inherit Service ID Value
- Service Name
- Description
- Service Tier
- Service Priority
- Administrative State
- Automatic SDP Binding/PBB Tunnel Creation

The Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.

The SVC Mgr Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.

The Default VC ID parameter is configurable when the Inherit Service ID Value parameter is disabled.

5 Configure the OLC state:

i Click on the Apply button.

ii Configure the parameters:

- Current OLC State
- Revert OLC State

6 If you enabled the Automatic SDP Binding/PBB Tunnel Creation parameter in step 4, perform the following steps. Otherwise, go to step 7.

i Click on the Select button beside the Profile Name parameter. The Select Tunnel Selection Profile - Epipe Service - Subscriber form opens.

ii Choose a tunnel selection profile from the list and click on the OK button. The Select Tunnel Selection Profile - Epipe Service - Subscriber form closes and the Epipe Service (Create) form refreshes with the tunnel selection profile information.

iii Configure the Transport Type parameter.

The Transport Type parameter is configurable only when the Profile Name parameter is not configured.

7 To configure AA reporting parameters for the 5670 RAM, perform the following steps.

i Click on the Application Assurance tab. The 5670 RAM Parameters tab is displayed.

ii Configure the parameters:

- Enable Application Performance Reporting
- Report Customer Name
- Number of IP Detail Addresses

iii To configure one or more custom DCP groups, see the custom DCP group configuration procedure in chapter 76.

iv To specify an application or application group for IP detail reporting, click on the IP Detail Application or IP Detail Application Group tab, as required. The IP Detail Application or IP Detail Application Group (Create) form opens.

Otherwise, go to step 8.

v Configure the parameters:

- ID
- Auto-Assign ID

vi Click on the Select button and choose an application or application group from the Select Application or Select Application Group form.

vii Click on the OK button. The IP Detail Application or IP Detail Application Group (Create) form closes, and a dialog box appears.

viii Click on the OK button. The application or application group is listed on the Epipe Service (Create) form.

ix To specify another application or application group for IP detail reporting, repeat steps 7 iv to viii.



Note — You can specify up to 10 applications and up to 10 application groups.

8 To configure service tunnel required bandwidth for the service, perform the following.



Note — In order to configure service tunnel required bandwidth, you must enable multi-segment tunnel selection and service bandwidth management at the system level. For more information see the *5620 SAM System Administrator Guide*.

i Click on the Bandwidth tab.

ii Configure the Bandwidth Method parameter.

iii If the Bandwidth Method parameter is set to Input Manually or Calculate from SAPs, configure LSP Path Booking and Service Path Booking parameters.

iv If the Bandwidth Method parameter is set to Input Manually, enter a required bandwidth value for each CoS (see CoS 0 Bandwidth - CoS 7 Bandwidth).

9 Click on the OK button. The Epipe Service (Create) form closes.

You can use the topology maps to view the service. See chapter 6 for more information about service topology maps.

10 To create a site for the VLL service, perform Procedure 67-2. For information about how to add a GNE site to a VLL service, see Procedure 67-25.

Procedure 67-2 To create a VLL Epipe site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VLL service and click on the Properties button. The Epipe Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 On the navigation tree, right-click on Epipe Service and choose Create Epipe Site. The Select Network Elements - Epipe Service form opens with a list of available NEs.

5 Choose a site and click on the OK button. The Epipe Site (Create) form opens with the General tab displayed. If you are configuring a 7210 SAS site, go to step 6. Otherwise, go to step 7.

6 If you are configuring a 7210 SAS site, perform one of the following:

a Choose a 7210 SAS and click on the OK button. The Site (Create) form opens with the General tab displayed. Go to step 7.

b Choose a non-7210 SAS terminating site that is physically connected to the 7210 SAS by a port or a LAG and click on the OK button. The Epipe Site (Create) form opens with the General tab displayed. Go to step 7.



Note — The non-7210 SAS terminating sites typically are a 7450 ESS, 7750 SR, 7710 SR, or 7950 XRS.

7 Configure the parameters:

- Name
- Description
- MTU
- Administrative State
- Monitor Access Interface Operational State

8 Configure the NE-specific parameters, as shown in Table 67-6.

Table 67-6 NE-specific parameters

NE	Parameters	Dependencies
7450 ESS, 7710 SR, 7750 SR, 7950 XRS	• VLL Site Type • Per Service Hashing for LAG Enabled • Tunnel Fault Notification	The site must be terminating if connected to a 7210 SAS-E, 7210 SAS-M, 7210 SAS-T, or 7210 SAS-X. The Tunnel Fault Notification parameter is configurable on sites where the device has ports configured in access or hybrid mode with QinQ encapsulation. If you are configuring a tunnel facility MEP, the Tunnel Fault Notification parameter must be set to Accept, in order to accept the fault propagation from the tunnel facility MEP.
7210 SAS-D, 7210 SAS-E, 7210 SAS-M, 7210 SAS-T, 7210 SAS-X	• SAP Type	When you configure a 3-plus-tag Epipe service, you must set the SAP Type parameter to qinq-inner Tag-preserve. See Epipe (Ethernet VLL) in section 67.1for more information. See Procedures 67-4 and 67-27 for additional configuration requirements for a 3-plus-tag Epipe service.
7210 SAS-M (in network mode), 7210 SAS-X	• Enable MTU Check • PBB Epipe	No dependencies

9 Configure service tunnel required bandwidth for the site.



Note — In order to configure service tunnel bandwidth management, you must enable multi-segment tunnel selection and service bandwidth management at the system level. For more information see the *5620 SAM System Administrator Guide*.

i Click on the Bandwidth tab.

ii Enable the Override Service Configuration parameter.

iii Configure the Bandwidth Method parameter.

iv If the Bandwidth Method parameter is set to Input Manually, enter a required bandwidth value for each CoS (see CoS 0 Bandwidth - CoS 7 Bandwidth).

10 Click on the OK button. A dialog box appears. The Epipe Site (Create) form closes and the site object is added to the Epipe Service (Edit) form navigation tree.

11 Create an additional site for the VLL service, if required. Repeat steps 4 to 10.



Note — If you are configuring a VLL with spoke switching, you must configure a switching site and two or more terminating sites.

12 Click on the OK button. The Epipe Service (Edit) form closes.

13 Perform one of the following:

a Link the site to a Backbone VPLS. See Procedure 67-3.

b Create endpoints for a redundant VLL. Perform Procedure 67-26.



Note — Redundant VLL Epipe services are configurable on the 7705 SAR, 7450 ESS, 7750 SR, 7710 SR, and 7950 XRS.

c Create a spoke SDP binding for the site. See Procedure 67-4.



Note — Only a single, non-redundant spoke SDP binding can be configured on a PBB Epipe site.

d Create a spoke SDP FEC for the site. See Procedure 67-6.

e Create one or more L2 access interfaces for the VLL terminating site. See Procedure 67-27.



Note 1 — If you are configuring access dual-homing with local switching over PBB tunnels, you must configure two L2 access interfaces. The L2 access interfaces can be on LAGs that participate in the MC LAG, or they can be just regular or Ethernet tunnel access interfaces.

Note 2 — If the Use SAP Backbone MAC Address parameter is enabled on both B-Sites:

- MC-LAG access interfaces for the PBB Epipe local switching must be on IOM3 MDAs for the feature to work properly. There is no 5620 SAM or CLI validation.
- Other access interfaces may be on IOM1 or IOM2 MDAs.

Note 3 — If you configure an L2 access interface on a PBB Epipe site you cannot configure a spoke SDP binding on the same site. They are mutually exclusive.

Note 4 — When you configure a 3-plus-tag Epipe service, you must choose a port with QinQ encapsulation as one endpoint. When the other endpoint is an L2 access interface, you must choose a port with dot1q or QinQ encapsulation as the other L2 access interface. Both endpoints must be on the same site. See "Epipe (Ethernet VLL)" in section 67.1 for more information. See Procedures 67-4 and 67-27 for additional configuration requirements for a 3-plus-tag Epipe service.

Procedure 67-3 To link the Epipe service to a backbone VPLS site

To link the Epipe service to a backbone VPLS site, perform the following procedure. For additional information on Provider Backbone Bridging, see chapter 68.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VLL service and click on the Properties button. The Epipe Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 On the navigation tree, expand the Site icon, right-click the site on which you want to link the VPLS site, and choose Properties.The Epipe Site (Edit) form opens with the General tab displayed.

5 Click on the Backbone tab.



Note — On the 7210 SAS-M and 7210 SAS-X, the Backbone tab is configurable only if you enabled the PBB Epipe in Procedure 67-2.

6 Click on the Select button. The Select Backbone VPLS Site - Epipe Site form opens.

7 Click the Search button. A list of all the B-Sites that can be used by the Epipe is displayed.



Note — The B-Sites listed are only those that are on the same NE type as the Epipe site. See Procedure 68-60 for more information.

8 Choose a B-VPLS and click on the OK button. The Select Backbone VPLS Site - Epipe Site form closes and the Service ID of the chosen B-VPLS appears in the Backbone VPLS Site panel.



Note — The selection of a B-Site in this step must be repeated for both Epipe sites. You must select a B-Site that is on the same NE as the Epipe site.

9 In the PBB panel, configure the following parameters:

- ISID
- Inherit Service ID Value
- Destination MAC Address or MAC Name

The ISID parameter is configurable when the Inherit Service ID Value parameter is disabled.



Note 1 — The ISID parameter should be set to the same value for both Epipe sites you create for this service.

Note 2 — To select a previously created Mac Name, click on the Select button and select a MAC Name from the list in the Select MAC Destination MAC Address Alias form. See Procedure 13-15 for more information about how to create a MAC Name.

Note 3 — The Destination MAC Address or MAC Name parameter you set for this Epipe site should be the same as the Source MAC Address of the B-Site on the other node of the Epipe service you are creating.

10 Configure the Force Q Tag Forwarding parameter.

11 Click on the OK button. The Operational Destination MAC Address is updated with the configured Destination MAC Address or MAC Address associated with the selected MAC Name.

Procedure 67-4 To create a spoke SDP binding on a VLL Epipe site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VLL service and click on the Properties button. The Epipe Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Site object on the navigation tree, right-click on Spoke SDP Bindings, and choose Create Spoke SDP Binding. The Spoke SDP Binding (Create) form opens with the General tab displayed.

5 Perform one of the following to specify a destination NE for the spoke SDP binding:

a If the destination NE is a managed NE, choose from a list of managed NEs.

i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element - Spoke SDP Binding form opens.

ii Choose a destination NE and click on the OK button. The Select Destination Network Element - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the tunnel termination site (the destination NE) identifier displayed.

b If the destination NE is an unmanaged NE, specify the system ID for the Tunnel Termination Site parameter.

6 Configure the parameters:

- Description
- Auto-Assign ID
- VC ID
- VC Type
- VLAN VC Tag
- Ingress Label
- Egress Label
- Block On Peer Fault



Note 1 — The VC ID parameter is configurable when the Auto-Assign ID parameter is disabled.

Note 2 — The Block On Peer Fault parameter takes effect only when PW status signaling is enabled.

Note 3 — The Block On Peer Fault parameter is not configurable on a spoke SDP that is on an MC LAG or an endpoint.

When you configure a 3-plus-tag Epipe service, you must set the VC Type parameter to VLAN. You must configure the VLAN VC Tag parameter with the same value as the inner tag of the QinQ SAP on the service. See "Epipe (Ethernet VLL)" in section 67.1 for more information. See Procedures 67-2 and 67-27 for additional configuration requirements for a 3-plus-tag Epipe service.

7 Perform one of the following to specify a transport tunnel for the spoke SDP binding.

a Allow the 5620 SAM to configure the transport tunnel automatically by choosing a profile name. See Procedure 27-3 for more information about how to create a service tunnel profile.

i Enable the Auto-Select Transport Tunnel parameter.

ii Click on the Select button beside the Profile Name parameter. The Select Tunnel Selection Profile - Spoke SDP Binding form opens.

iii Choose a tunnel selection profile and click on the OK button. The Select Tunnel Selection Profile - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the profile name displayed.

b Allow the 5620 SAM to configure the transport tunnel automatically by choosing a transport encapsulation type.

i Enable the Auto-Select Transport Tunnel parameter.

ii Configure the Tunnel Auto-Selection Transport Preference parameter.

c Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens. See Procedure 27-1 for more information about how to create a service tunnel.

ii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier.



Note — The 5620 SAM blocks the manual selection of a tunnel with insufficient bandwidth if the server configuration includes the following parameter setting:

<vll-CAC enforceTunnelBandwidth="true"/>

The parameter is set to false by default, which means that the 5620 SAM does not block the manual selection of a tunnel with insufficient bandwidth; instead, the “Insufficient Bandwidth To Allocate To SDP Binding” State Cause indicator is set.

To change the parameter setting, contact Alcatel-Lucent technical support.

d Configure an MPLS-TP transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens.

ii Select an MPLS-TP service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier. See Procedure 27-1 for more information about how to create an MPLS-TP service tunnel.

8 If the Epipe service is linked to a Backbone VPLS go to step 10.

9 If you are creating redundant SDP bindings, configure the endpoint in the Redundancy panel:

i Click on the Select button in the Redundancy panel to select an endpoint for the transport tunnel. The drop-down menu displays the available endpoints.

ii Configure the parameters:

- Inter-Chassis Backup
- Precedence
- Active State

When the Precedence parameter is set to 0, you can configure a secondary SAP on an ATM interface, MC-APS, or APS for HSPDA offload fallback.

10 Configure the parameters:

- Enable Hash Label
- Enable Signal Capability
- Force VLAN VC Forwarding
- SDP Admin Bandwidth
- Enable PW Status Signaling
- Enable PW Standby Signaling Slave

The Enable Signal Capability parameter is configurable when the Enable Hash Label parameter is enabled.



Note 1 — If you are creating an Epipe service linked to a Backbone VPLS, then the Enable PW Status Signaling and Enable PW Standby Signaling Slave parameters are not be configurable.

Note 2 — The Enable Hash Label, Enable PW Status Signaling, and SDP Admin Bandwidth parameters are not configurable if you selected an MPLS-TP tunnel in step 7.

11 Perform one of the following to specify a transport tunnel for the Return SDP binding, if required.



Note 1 — You can create a return tunnel only between sites that are in the same service. If the sites are not in the same service, the Return tab does not appear.

Note 2 — When the Auto Select Return Transport Tunnel parameter is enabled, 5620 SAM will consider and use a portion of the bandwidth you specified when setting the SDP Admin Bandwidth parameter in step 10.

a Allow the 5620 SAM to configure the transport tunnel automatically by choosing a profile name. See Procedure 27-3 for more information about how to create a service tunnel profile.

i Click on the Return tab.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Click on the Select button beside the Profile Name parameter. The Select Return Tunnel Selection Profile - Spoke SDP Binding form opens.

iv Choose a tunnel selection profile and click on the OK button. The Select Return Tunnel Selection Profile - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the profile name displayed.

b Allow the 5620 SAM to configure the transport tunnel automatically by choosing a transport encapsulation type.

i Click on the Return tab.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Configure the Return Tunnel Auto-Selection Transport Preference parameter.

c Configure the transport tunnel manually.

i Click on the Return tab.

ii Click on the Select button in the Return Tunnel panel. The Select Return Tunnel - Spoke SDP Binding form opens. See Procedure 27-1 for more information about how to create a service tunnel

iii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Return Tunnel - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the service Tunnel ID, Name, and Underlying Transport displayed in the Tunnel panel.

12 Click on Select in the Return SDP Binding Endpoint panel to choose a Return Endpoint on the terminating site. Select the required endpoint from the drop-down list.

13 Choose an Application Profile for the spoke SDP binding. See Procedure 76-1 for more information about how to configure an application profile.

i Click on the General tab.

ii Click on the Select button beside the Application Profile parameter. The Application Profile String: - Spoke SDP Binding form opens.

iii Configure the filter criteria and click on the Search button. A list of Application Profiles appears.

iv Choose an application profile from the list and click on the OK button. The Application Profile String: - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the application profile displayed.



Note — The Application Profile String: - Spoke SDP Binding - VLL service form displays only local profiles on the NE.

14 Associate an AA transit prefix policy with the service object, if required. See Procedure 76-10 for more information about how to configure a transit prefix policy.

i Click on the Select button in the Transit Prefix Policy panel. The Select Transit Prefix Policy - Spoke SDP Binding form opens.

ii Select a transit IP policy and click on the OK button. The Select Transit Prefix Policy - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the transit prefix policy ID displayed.

15 To configure custom object attributes for AA reporting to the 5670 RAM, perform the following steps:

i Click on the 5670 RAM Parameters tab.

ii Click on the Reporting tab.

iii Click on the Create button. The AA Reporting (Create) form opens.

iv Configure the parameters:

- Customer Name
- Subscriber Class
- Total Bandwidth Upstream (Kbps)
- Class of Service 1 Bandwidth Upstream (Kbps)
- Class of Service 2 Bandwidth Upstream (Kbps)
- Class of Service 3 Bandwidth Upstream (Kbps)
- Class of Service 4 Bandwidth Upstream (Kbps)
- Subscriber Name
- Subscriber Type
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)

v Click on the OK button. The AA Reporting (Create) form closes and the reporting object is displayed in the list.

16 Click on the QoS tab.

17 Configure the required parameters in the Forwarding Plane Redirect panel:

i Click on the Network Policy Select button to assign a policy to the Spoke SDP Binding. The Select Network Policy - Spoke SDP Binding form opens.



Note — To create a network policy, click on the Create button and perform Procedure 43-6.

ii Choose a policy from the list and click on the OK button. The Network Policy form closes and the QoS tab refreshes with the policy name displayed.

iii Click on the Ingress Queue Group Template Policy Select button to assign a policy to the Spoke SDP Binding. The Select Ingress Queue Group Template Policy form opens.



Note — To create an ingress queue group template policy, click on the Create button and perform Procedure 43-23.

iv Choose a policy from the list and click on the OK button. The Ingress Queue Group Template Policy form closes and the QoS tab refreshes with the policy name displayed.

v Configure the Instance ID parameter.

18 Configure the required parameters in the Port Redirect panel:

i Click on the Network Policy Select button to assign a policy to the Spoke SDP Binding. The Select Network Policy form opens.



Note — To create a network policy, click on the Create button and perform Procedure 43-6.

ii Choose a policy from the list and click on the OK button. The Network Policy form closes and the QoS tab refreshes with the policy name displayed.

iii Click on the Egress Queue Group Template Policy Select button to assign a policy to the Spoke SDP Binding. The Select Egress Queue Group Template Policy form opens.



Note — To create an egress queue group template policy, click on the Create button and perform Procedure 43-24.

iv Choose a policy from the list and click on the OK button. The Egress Queue Group Template Policy form closes.

v Configure the Instance ID parameter.

19 Click on the States tab and configure the Administrative State parameter.

20 Click on the Pseudowire OAM tab and configure the Control Word parameter.



Note — If you are creating a spoke SDP binding using an MPLS-TP service tunnel for pseudowire static configuration, you must set the Control Word parameter to Preferred.

21 Assign ingress and egress filter policies to the spoke SDP binding, if required. See chapter 44 for more information about how to configure filter policies.

i Click on the ACL tab.

ii Click on the Select button in the *[filter policy type]* Ingress Filter panel to choose an ingress filter policy. The Select Ingress Filter - Spoke SDP Binding form opens.

iii Choose an ingress filter and click on the OK button. The Select Ingress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form reappears with the ingress filter policy information displayed.

iv Click on the Select button in the *[filter policy type]* Egress Filter panel to choose an egress filter policy. The Select Egress Filter - Spoke SDP Binding form opens.

v Choose an egress filter policy and click on the OK button. The Select Egress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form reappears with the egress filter policy information displayed.

vi Repeat steps ii to v for each filter policy type, as required.

22 Assign an accounting policy to the SDP binding, if required.



Note — To create an accounting policy, click on the Create button and perform see the accounting statistics collection chapter in the *5620 SAM Statistics Management Guide*.

i Click on the Accounting tab.

ii Configure the Collect Accounting Statistics parameter.

iii Click on the Select button to choose an accounting policy. The Select Accounting Policy - Spoke SDP Binding form opens.

iv Choose an accounting policy and click on the OK button. The Select Accounting Policy - Spoke SDP Binding form closes and the Spoke SDP Binding form reappears with the accounting policy information displayed.

23 Associate a MEP to the spoke SDP binding, if required.

i Click on the ETH-CFM tab.

ii Configure the parameters in the MIP panel:

- MIP
- MIP MAC Address

iii Click on the Create button. The MEP (Create) form opens on the General tab.

iv Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

v Choose an entry and click on the OK button. The Select Maintenance Entity Group form closes.

vi Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Propagation
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)
- CCM Padding Packet Size(Bytes)



Note — The CCM Padding Packet Size(Bytes) parameter cannot be configured when the CCM interval parameter is set to 10 ms or 100 ms.

vii If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab. Otherwise, go to step xi.

viii Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

ix Click on the AIS tab.

x Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

xi Click on the OK button. A dialog box appears.

xii Click on the OK button. The MEP (Create) form closes.

24 Click on the OK button. The Spoke SDP Binding (Create) form closes and a dialog box appears.

25 Click on the OK button. The Epipe Service (Edit) form reappears with the new spoke SDP binding information displayed in the service navigation tree.

26 Perform one of the following:

a If you are configuring a VLL with spoke switching, you must configure a switching site and two or more terminating sites. Repeat Procedure 67-2 to configure more sites, and repeat steps 4 through 25 of this procedure, as required.

b If you are configuring a PBB Epipe, you can only configure one Spoke SDP. Go to step 27.

27 Click on the OK button. A dialog box appears.

28 Click on the OK button. The Epipe Service (Edit) form closes.

Procedure 67-5 To configure an MPLS-TP static pseudowire on an Epipe spoke SDP binding

Perform this procedure to create an MPLS-TP static pseudowire on the spoke SDP binding. An MPLS-TP service tunnel must be used in the SDP binding, and the Control Word parameter for pseudowire OAM must be set to Preferred. See Procedure 67-4.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Select an Epipe and click on the Properties button. The Epipe Service (Edit) form opens.

4 On the navigation tree, expand the site on which you want to configure the spoke SDP binding, and expand the Spoke SDP Bindings icon.

5 Click on the SDP binding on which you want to configure the MPLS-TP static pseudowire. The Spoke SDP Binding (Edit) form opens with the General tab displayed.

6 Click on the Control Channel tab.

7 Configure the parameters:

- Status
- Refresh Timer (seconds)

8 Click on the MPLS-TP PW tab.

9 Click on the Create button. The PW Path ID (Create) form opens.

10 Configure the Path AGI parameter.

11 Configure the parameters in the Source Attachment Individual Identifier panel:

- SAII Global ID
- SAII Node ID
- SAII AC ID

12 Configure the parameters in the Target Attachment Individual Identifier panel:

- TAII Global ID
- TAII Node ID
- TAII AC ID

13 Click on the OK button. The PW Path ID (Create) form closes.

14 Click on the OK button. The Spoke SDP Binding (Edit) form closes.

15 Close the Epipe Service (Edit) form.

16 Close the Manage Services form.

Procedure 67-6 To create a spoke SDP FEC binding on a VLL Epipe site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VLL service and click on the Properties button. The Epipe Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 On the navigation tree, right-click on Spoke SDP FECs and choose Create Spoke SDP FEC. The Spoke SDP FEC (Create) form opens.

5 Configure the parameters:

- PW ID
- Auto-Assign ID

6 In the Source panel, perform the following:

i Click on the Select button beside the SAII Address field and select an SAII address.

ii Configure the SAII AC ID parameter. See chapter 72 for SAII configuration information.

7 In the Target panel, perform one of the following:

a Configure the Auto Config parameter.

b Perform the following:

i Click on the Select button beside the TAII Address field and select a TAII address.

ii Configure the TAII AC ID parameter. See chapter 72 for SAII configuration information.

8 In the General Parameters panel, perform the following:

i Configure the parameters.

- Administrative State
- Signalling Type
- Retry Timer
- Retry Counter

ii Click on the Select button beside the Path field. The Select Path - Spoke SDP FEC form opens.

iii Click on the Search button and select a path.

iv Click on the OK button. The Select Path - Spoke SDP FEC form closes.

v Click on the Select button beside the PW Template field. The Select PW Template - Spoke SDP FEC form opens.

vi Click on the Search button and select a template.

vii Click on the OK button. The Select PW Template - Spoke SDP FEC form closes.

9 On the Redundancy panel, perform the following:

i Click on the Select button beside the Endpoint field and select an endpoint.

ii Configure the parameters:

- Inter-Chassis Backup
- Precedence
- Active State

10 On the Pseudowire Signalling panel, configure the Enable PW Standby Signaling Slave parameter.

11 Click on the OK button. A dialog box appears and the Epipe Service (Edit) form reappears with the new spoke SDP binding information displayed in the service navigation tree.

12 Click on the OK button. The Epipe Service (Edit) form closes.

Procedure 67-7 To configure an Epipe site for BGP multi-homing

This procedure provides the steps required to configure an Epipe site for BGP multi-homing. Configuring Epipe sites in this way allows for multi-homed connectivity to G.8031 Ethernet tunnels between two CEs. G.8031 resiliency is used on the edges and then pseudowires are allowed to reach the far end, where G.8031 can again be used in a multi-chassis mode.

G.8031 is created on two CEs which are multi-homed to two PEs. Using BGP and CFM, PE routers enable or disable the CE-PE SAPs. The core is IP/MPLS and Epipe is used for transport between the PEs. The Ethernet tunnels are created on the CEs and the Epipe service on the CEs uses these tunnels.

1 Before you configure a site for BGP multi-homing, you must perform the following:

a Enable BGP on the routing instance of each NE in the Epipe BGP multi-homing configuration. See Procedure 23-1 for more information.

b Configure global-level BGP on each NE in the Epipe BGP multi-homing configuration. See Procedure 23-2 for more information. The following items are required:

- Enable the L2 VPN parameter on:
  - the VPN tab of the BGP site form
  - the VPN tab of the BGP Peer Group form, which contains the peers that are involved in the BGP multi-homing
- Create a peer group under BGP. This peer group is used to collectively define the peers involved in the Epipe BGP multi-homing configuration.
- Create the required peers under the peer group. These peers are the NEs involved in the Epipe BGP multi-homing configuration.



Note — For optimal processing while a BGP multi-homing site is activated or de-activated, or the system is rebooted, you should also:

- Enable the L2 VPN parameter in the Rapid Update Address Family panel on the BGP site VPN tab.
- Enable the Enable Rapid Withdrawal parameter on the BGP site Behavior tab.

2 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

3 Configure the filter criteria and click the Search button. A list of services appears.

4 Select the required Epipe service and click on the Properties button. The Epipe Service (Edit) form opens with the General tab displayed.

5 Perform one of the following:

a On the navigation tree, right-click on the required site and choose Properties. The Epipe Site (Edit) form opens with the General tab displayed.



Note — You can see a list of all current Epipe multi-homing service sites by viewing the BGP Multi-homing tab on the service configuration form.

b Create a new site. Perform steps 4 to 10 in Procedure 67-2.

6 Click on the BGP tab.

7 Enable the Enable BGP parameter. The RD and RT panels are displayed.

8 Configure the Route Distinguisher parameter in the RD panel. Enabling the Show Format checkbox displays a list of acceptable formats and value ranges.



Note — An RD or RT configured under the BGP of an Epipe site cannot be removed as long as there is a multi-homing site configured that uses these and whose administration state is up.

9 Configure the Import Route Target and Export Route Target parameters in the RT panel. Enabling the Show Format checkbox displays a list of acceptable formats and value ranges.

You can also configure the Export Route Target to be the same as the Import Route Target by enabling the Same as Import checkbox.

10 Click on the Multi-homing sub-tab.

11 Click on the Create button. The BGP Multi-homing Site (Create) form opens.

12 Configure the parameters:

- Multi-homing Site Name
- Multi-homing ID
- Site Preference



Note — You cannot turn up a BGP multi-homing site without specifying a Multi-homing ID. In addition, the site's Multi-homing ID can only be removed at a later time when the site is shutdown.

13 Click the Select button to specify a SAP for the BGP multi-homing. The Select L2 Access Interface form is displayed.



Note — You cannot turn up a BGP multi-homing site without specifying a SAP. The SAP configured under this site can be part of an endpoint, but the only other object allowed in the endpoint is an ICB spoke-SDP. In addition, an assigned SAP can only be removed at a later time when the BGP multi-homing site is shutdown.

14 Click the Search button to display a list of eligible SAPs.

15 Select the required SAP and click OK. The Select L2 Access Interface form closes and the BGP Multi-homing Site (Create) form is refreshed to display the selected SAP.

16 Configure the parameters:

- Use Node Level Boot Timer
- Boot Timer (seconds)
- Use Node Level Site Activation Timer
- Activation Timer (seconds)
- Administrative State

If you enable either the Use Node Level Boot Timer and/or Use Node Level Site Activation Timer parameters, then the associated Boot Timer (seconds) and/or Activation Timer (seconds) parameters will not be configurable. These parameter values will be inherited from the network element configuration.

The Boot Timer (seconds) and Activation Timer (seconds) parameters can be configured for an NE on the BGP Multi-homing sub-tab under the Redundancy tab in the Network Element (Edit) form. See Procedure 13-2 for more information on changing device properties.

17 Click on the OK button. The BGP Multi-homing Site (Create) form closes.

18 Close the Epipe Service (Edit) form.

Procedure 67-8 To create a VLL Apipe service

VLL Apipe services are configurable only on the 7450 ESS in mixed mode, 7750 SR, 7710 SR, 7950 XRS, and 7705 SAR.

1 Choose Create→Service→VLL→Apipe (ATM to ATM/FR) from the 5620 SAM main menu. The Apipe Service (Create) form opens.

2 Click on the Select button to choose a customer to associate with the VLL service. The Select Customer - Apipe Services form opens.

3 Choose a customer for the VLL service and click on the OK button. The Select Customer - Apipe Service form closes and the Apipe Service (Create) form refreshes with the customer information

4 Configure the parameters:

- Service ID
- Auto-Assign ID
- SVC Mgr Service ID
- Default VC ID
- Inherit Service ID Value
- Service Name
- Description
- Service Tier
- Service Priority
- Administrative State
- VC Type
- Automatic SDP Binding/PBB Tunnel Creation

The Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.

The SVC Mgr Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.

The Default VC ID parameter is configurable when the Inherit Service ID Value parameter is disabled.

5 Configure the OLC state:

i Click on the Apply button.

ii Configure the parameters:

- Current OLC State
- Revert OLC State

6 If you enabled the Automatic SDP Binding/PBB Tunnel Creation parameter in step 4, perform the following steps. Otherwise, go to step 7.

i Click on the Select button beside the Profile Name parameter. The Select Tunnel Selection Profile - Apipe Service - Subscriber form opens.

ii Choose a tunnel selection profile from the list and click on the OK button. The Select Tunnel Selection Profile - Apipe Service - Subscriber form closes and the Apipe Service (Create) form refreshes with the tunnel selection profile information.

iii Configure the Transport Type parameter. The Transport Type parameter is configurable only when the Profile Name parameter is not configured.

7 To configure service tunnel required bandwidth for the service, perform the following steps.



Note — In order to configure service tunnel required bandwidth, you must enable multi-segment tunnel selection and service bandwidth management at the system level. For more information see the *5620 SAM System Administrator Guide*.

i Click on the Bandwidth tab.

ii Configure the Bandwidth Method parameter.

iii If the Bandwidth Method parameter is set to Input Manually or Calculate from SAPs, configure LSP Path Booking and Service Path Booking parameters.

iv If the Bandwidth Method parameter is set to Input Manually, enter a required bandwidth value for each CoS (see CoS 0 Bandwidth - CoS 7 Bandwidth).

8 Click on the OK button. The Apipe Service (Create) form closes.

9 To create a site for the VLL, perform Procedure 67-9.

For information on adding a GNE site to a VLL service, see Procedure 67-25.

10 If required, modify the SDP binding parameters for ATM cell concatenation.

i Open and modify the Apipe configuration form, as described in Procedure 67-51.

ii Click on the Spoke SDP Binding tab.

iii Choose a SDP binding from the list and click on the Properties button.

iv Click on the ATM tab.

v Configure the parameters:

- AAL5 Frame Aware
- Admin Concat Limit
- Max Concat Delay
- CLP Change

vi Save the changes and close the Apipe configuration form.

Procedure 67-9 To create a VLL Apipe site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VLL service and click on the Properties button. The Apipe Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 On the navigation tree, right-click on Apipe Service and choose Create Apipe Site. The Select Network Elements - Apipe Service form opens with a list of available NEs.

5 Choose a site and click on the OK button. The Site (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Name
- Description
- MTU
- Administrative State
- Monitor Access Interface Operational State
- Interworking Type
- Signalling VC Type Override

7 Configure the NE-specific parameters, as shown in Table 67-7.

Table 67-7 NE-specific parameters

NE	Parameters	Dependencies
7450 ESS, 7750 SR, 7705 SAR	VLL Site Type	The VLL Site Type parameter is displayed as read-only for the 7950 XRS, as only switching VLL sites are supported.

8 To configure service tunnel required bandwidth for the site, perform the following steps.



Note — In order to configure service tunnel required bandwidth, you must enable multi-segment tunnel selection and service bandwidth management at the system level. For more information see the *5620 SAM System Administrator Guide*.

i Click on the Bandwidth tab.

ii Enable the Override Service Configuration parameter.

iii Configure the Bandwidth Method parameter.

iv If the Bandwidth Method parameter is set to Input Manually, enter a required bandwidth value for each CoS (see CoS 0 Bandwidth - CoS 7 Bandwidth).

9 Click on the OK button. The Apipe Site (Create) form closes.

10 Perform one of the following:

a Create endpoints for a redundant VLL. Perform Procedure 67-26.



Note — Redundant VLL Apipe services are configurable on the 7450 ESS, 7705 SAR, 7710 SR, 7950 XRS, and 7750 SR.

b Create an L2 access interface for the VLL terminating site. Perform Procedure 67-27.

c Create a SAP aggregation group with L2 access interfaces for the VLL terminating sites. See Procedure 67-43.

d Create a spoke SDP binding for the site. Perform Procedure 67-10.

11 Create an additional site for the VLL service, if required. Repeat steps 4 to 9.

Procedure 67-10 To create a spoke SDP binding on a VLL Apipe site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VLL service and click on the Properties button. The Apipe Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 On the navigation tree, expand the Site object and right-click on Spoke SDP Bindings and choose Create Spoke SDP Binding. The Spoke SDP Binding (Create) form opens with the General tab displayed.

5 Specify a destination NE for the spoke SDP binding:

a If the destination NE is a managed NE, choose from a list of managed NEs.

i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element - Spoke SDP Binding form opens.

ii Choose a destination NE and click on the OK button. The Select Destination Network Element - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the tunnel termination site (the destination NE) identifier displayed.

b If the destination NE is an unmanaged NE, specify the system ID for the Tunnel Termination Site parameter.

6 Configure the parameters:

- Description
- Auto-Assign ID
- VC ID
- Ingress Label
- Egress Label
- SDP Admin Bandwidth

The VC ID parameter is configurable when the Auto-Assign ID parameter is disabled.



Note — The SDP Admin Bandwidth parameter is not configurable if you select an MPLS-TP tunnel in step 7.

7 Perform one of the following to specify a transport tunnel for the spoke SDP binding.

a Allow the 5620 SAM to configure the transport tunnel automatically by choosing a profile name. See Procedure 27-3 for more information about how to create a service tunnel profile.

i Enable the Auto-Select Transport Tunnel parameter.

ii Click on the Select button beside the Profile Name parameter. The Select Tunnel Selection Profile - Spoke SDP Binding form opens.

iii Choose a tunnel selection profile and click on the OK button. The Select Tunnel Selection Profile - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the profile name displayed.

b Allow the 5620 SAM to configure the transport tunnel automatically by choosing a transport encapsulation type.

i Enable the Auto-Select Transport Tunnel parameter.

ii Configure the Tunnel Auto-Selection Transport Preference parameter.

c Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens. See Procedure 27-1 for more information about how to create a service tunnel.

ii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier.



Note — The 5620 SAM blocks the manual selection of a tunnel with insufficient bandwidth if the server configuration includes the following parameter setting:

<vll-CAC enforceTunnelBandwidth="true"/>

The parameter is set to false by default, which means that the 5620 SAM does not block the manual selection of a tunnel with insufficient bandwidth; instead, the “Insufficient Bandwidth To Allocate To SDP Binding” State Cause indicator is set.

To change the parameter setting, contact Alcatel-Lucent technical support.

d Configure an MPLS-TP transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens.

ii Select an MPLS-TP service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier. See Procedure 27-1 for more information about how to create an MPLS-TP service tunnel.

8 If you are creating redundant SDP bindings, configure the endpoint in the Redundancy panel:

i Click on the Select button in the Redundancy panel to select an endpoint for the transport tunnel. The drop-down menu displays the available endpoints.

ii Configure the parameters:

- Inter-Chassis Backup
- Precedence

  If you set this parameter to 0, you can configure a secondary SAP on an ATM interface, MC-APS, or APS for HSPDA offload fallback.
- Active State

9 Perform one of the following to specify a transport tunnel for the Return SDP binding, if required.



Note 1 — You can create a return tunnel only between sites that are in the same service. If the sites are not in the same service, the Return tab does not appear.

Note 2 — When the Auto Select Return Transport Tunnel parameter is enabled, 5620 SAM will consider and use a portion of the bandwidth you specified when setting the SDP Admin Bandwidth parameter in step 6.

a Allow the 5620 SAM to configure the transport tunnel automatically by choosing a profile name. See Procedure 27-3 for more information about how to create a service tunnel profile.about how to create a service tunnel profile.

i Click on the Return tab.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Click on the Select button beside the Profile Name parameter. The Select Return Tunnel Selection Profile - Spoke SDP Binding form opens.

iv Choose a tunnel selection profile and click on the OK button. The Select Return Tunnel Selection Profile - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the profile name displayed.

b Allow the 5620 SAM to configure the transport tunnel automatically by choosing a transport encapsulation type.

i Click on the Return tab.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Configure the Return Tunnel Auto-Selection Transport Preference parameter.

c Configure the transport tunnel manually.

i Click on the Return tab.

ii Click on the Select button in the Return Tunnel panel. The Select Return Tunnel - Spoke SDP Binding form opens. See Procedure 27-1 for more information about how to create a service tunnel.

iii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Return Tunnel - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the service Tunnel ID, Name, and Underlying Transport displayed in the Tunnel panel.

10 Click on Select in the Return SDP Binding Endpoint panel to choose a Return Endpoint on the terminating site. Select the required endpoint from the drop-down list that appears.

11 Click on the States tab.

12 Configure the Administrative State parameter.

13 Click on the Pseudowire OAM tab.

14 Configure the Control Word parameter.

If you set the VC Type parameter to ATM-SDU in step 4 of Procedure 67-8, you must set the Control Word parameter to Preferred.

15 Click on the OK button. The Spoke SDP Binding (Create) form closes and a dialog box appears.

16 Click on the OK button. The Apipe Site (Edit) form reappears with the new spoke SDP binding information displayed in the service navigation tree.

17 Click on the OK button. The Apipe Site (Edit) form closes and a dialog box appears.

18 Click on the OK button. The Apipe Service (Edit) form reappears.

19 Close the Apipe Service (Edit) form.

Procedure 67-11 To configure an MPLS-TP static pseudowire on an Apipe spoke SDP binding

Perform this procedure to create an MPLS-TP static pseudowire on the spoke SDP binding. An MPLS-TP service tunnel must be used in the SDP binding, and the Control Word parameter for pseudowire OAM must be set to Preferred. See Procedure 67-10.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Select an Epipe and click on the Properties button. The Apipe Service (Edit) form opens.

4 On the navigation tree, expand the site on which you want to configure the spoke SDP binding, and expand the Spoke SDP Bindings icon.

5 Click on the SDP binding on which you want to configure the MPLS-TP static pseudowire. The Spoke SDP Binding (Edit) form opens with the General tab displayed.

6 Click on the Control Channel tab.

7 Configure the parameters:

- Status
- Refresh Timer (seconds)
- Request Timer (seconds)
- Retry Timer (seconds)
- Timeout Multiplier
- Acknowledged

8 Click on the MPLS-TP PW tab.

9 Click on the Create button. The PW Path ID (Create) form opens.

10 Configure the Path AGI parameter.

11 Configure the parameters in the Source Attachment Individual Identifier panel:

- SAII Global ID
- SAII Node ID
- SAII AC ID

12 Configure the parameters in the Target Attachment Individual Identifier panel:

- TAII Global ID
- TAII Node ID
- TAII AC ID

13 Click on the OK button. The PW Path ID (Create) form closes.

14 Click on the OK button. The Spoke SDP Binding (Edit) form closes.

15 Close the Apipe Service (Edit) form.

16 Close the Manage Services form.

Procedure 67-12 To create a VLL Fpipe service

1 Choose Create→Service→VLL→Fpipe (FR to FR) from the 5620 SAM main menu. The Fpipe Service (Create) form opens.

2 Click on the Select button to choose a customer to associate with the VLL service. The Select Customer - Fpipe Service form opens. See Procedure 64-1for information about how to create a customer.

3 Choose a customer for the VLL service and click on the OK button. The Select Customer - Fpipe Service form closes and the Fpipe Service (Create) form refreshes with the customer information displayed.

4 Configure the parameters:

- Service ID
- Auto-Assign ID
- SVC Mgr Service ID
- Default VC ID
- Inherit Service ID Value
- Service Name
- Description
- Service Tier
- Service Priority
- Administrative State
- VC Type
- Automatic SDP Binding/PBB Tunnel Creation

The Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.

The SVC Mgr Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.

The Default VC ID parameter is configurable when the Inherit Service ID Value parameter is disabled.

5 Configure the OLC state:

i Click on the Apply button.

ii Configure the parameters:

- Current OLC State
- Revert OLC State

6 If you enabled the Automatic SDP Binding/PBB Tunnel Creation parameter in step 4, perform the following steps. Otherwise, go to step 7.

i Click on the Select button beside the Profile Name parameter. The Select Tunnel Selection Profile - Fpipe Service - Subscriber form opens.

ii Choose a tunnel selection profile from the list and click on the OK button. The Select Tunnel Selection Profile - Fpipe Service - Subscriber form closes and the Fpipe Service (Create) form refreshes with the tunnel selection profile information.

iii Configure the Transport Type parameter. The Transport Type parameter is configurable only when the Profile Name parameter is not configured.

7 To configure service tunnel required bandwidth for the service, perform the following steps.



Note — In order to configure service tunnel required bandwidth, you must enable multi-segment tunnel selection and service bandwidth management at the system level. For more information see the *5620 SAM System Administrator Guide*.

i Click on the Bandwidth tab.

ii Configure the Bandwidth Method parameter.

iii If the Bandwidth Method parameter is set to Input Manually or Calculate from SAPs, configure LSP Path Booking and Service Path Booking parameters.

iv If the Bandwidth Method parameter is set to Input Manually, enter a required bandwidth value for each CoS (see CoS 0 Bandwidth - CoS 7 Bandwidth).

8 Perform one of the following:

a Create a site for the VLL. Perform Procedure 67-13.

b Complete VLL creation if sites and interfaces are to be created later. Go to step 9.

For information on adding a GNE site to a VLL service, see Procedure 67-25.

9 Click on the OK button. A dialog box appears.

10 Click on the OK button. The Fpipe Service (Create) form reappears.

11 Click on the OK button. The Fpipe Service (Create) form closes.

You can use the service topology maps to view the service. See chapter 6 for more information about service topology maps.

12 Perform one of the following:

a Create endpoints for a redundant VLL. Perform Procedure 67-26.

b Create an L2 access interface for the VLL terminating site. Perform Procedure 67-27.

c Create a spoke SDP binding for the site. Perform Procedure 67-14.

Procedure 67-13 To create a VLL Fpipe site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VLL service and click on the Properties button. The Fpipe Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 On the navigation tree, right-click on Fpipe Service and choose Create Fpipe Site. The Select Network Elements - Fpipe Service form opens with a list of available NEs.

5 Choose a site and click on the OK button. The Site (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Name
- Description
- MTU
- Administrative State
- Monitor Access Interface Operational State

7 Configure the NE-specific parameters, as shown in Table 67-8.

Table 67-8 NE-specific parameters

NE	Parameters	Dependencies
7450 ESS, 7750 SR, 7705 SAR	VLL Site Type	No dependencies

8 To configure service tunnel required bandwidth for the site, perform the following steps.



Note — In order to configure service tunnel required bandwidth, you must enable multi-segment tunnel selection and service bandwidth management at the system level. For more information see the *5620 SAM System Administrator Guide*.

i Click on the Bandwidth tab.

ii Enable the Override Service Configuration parameter.

iii Configure the Bandwidth Method parameter.

iv If the Bandwidth Method parameter is set to Input Manually, enter a required bandwidth value for each CoS (see CoS 0 Bandwidth - CoS 7 Bandwidth).

9 Click on the OK button. The Fpipe Site (Create) form closes.

10 Create an additional site for the VLL service, if required. Repeat steps 4 to 9.

11 Perform one of the following:

a Create endpoints for a redundant VLL. Perform Procedure 67-26.



Note — Redundant VLL Apipe services are configurable on the 7450 ESS, 7705 SAR, 7710 SR, and 7750 SR.

b Create an L2 access interface for the VLL terminating site. Perform Procedure 67-27.

c Create a SAP aggregation group with L2 access interfaces for the VLL terminating sites. See Procedure 67-43.

d Create a spoke SDP binding for the site. Perform Procedure 67-14.

Procedure 67-14 To create a spoke SDP binding on a VLL Fpipe site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VLL service and click on the Properties button. The Fpipe Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 On the navigation tree, right-click on Spoke SDP Bindings and choose Create Spoke SDP Binding. The Spoke SDP Binding (Create) form opens with the General tab displayed.

5 Specify a destination NE for the spoke SDP binding:

a If the destination NE is a managed NE, choose from a list of managed NEs.

i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element - Spoke SDP Binding form opens.

ii Choose a destination NE and click on the OK button. The Select Destination Network Element - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the tunnel termination site (the destination NE) identifier displayed.

b If the destination NE is an unmanaged NE, specify the system ID for the Tunnel Termination Site parameter.

6 Configure the parameters:

- Description
- Auto-Assign ID
- VC ID
- Ingress Label
- Egress Label

The VC ID parameter is configurable when the Auto-Assign ID parameter is disabled.

7 Perform one of the following to specify a transport tunnel for the spoke SDP binding.

a Allow the 5620 SAM to configure the transport tunnel automatically by choosing a profile name. See Procedure 27-3 for more information about how to create a service tunnel profile.

i Enable the Auto-Select Transport Tunnel parameter.

ii Click on the Select button beside the Profile Name parameter. The Select Tunnel Selection Profile - Spoke SDP Binding form opens.

iii Choose a tunnel selection profile and click on the OK button. The Select Tunnel Selection Profile - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the profile name displayed.

b Allow the 5620 SAM to configure the transport tunnel automatically by choosing a transport encapsulation type.

i Enable the Auto-Select Transport Tunnel parameter.

ii Configure the Tunnel Auto-Selection Transport Preference parameter.

c Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens. See Procedure 27-1 for more information about how to create a service tunnel.

ii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier.



Note — The 5620 SAM blocks the manual selection of a tunnel with insufficient bandwidth if the server configuration includes the following parameter setting:

<vll-CAC enforceTunnelBandwidth="true"/>

The parameter is set to false by default, which means that the 5620 SAM does not block the manual selection of a tunnel with insufficient bandwidth; instead, the “Insufficient Bandwidth To Allocate To SDP Binding” State Cause indicator is set.

To change the parameter setting, contact Alcatel-Lucent technical support.

8 If you are creating redundant SDP bindings, configure the endpoint in the Redundancy panel:

i Click on the Select button in the Redundancy panel to select an endpoint for the transport tunnel. The drop-down menu displays the available endpoints.

ii Configure the parameters:

- Inter-Chassis Backup
- Precedence
- Active State

9 Configure the parameters:

- Enable Hash Label
- Enable Signal Capability
- SDP Admin Bandwidth

The Enable Signal Capability parameter is configurable when the Enable Hash Label is enabled.

10 Perform one of the following to specify a transport tunnel for the Return SDP binding, if required.



Note 1 — You can create a return tunnel only between sites that are in the same service. If the sites are not in the same service, the Return tab does not appear.

Note 2 — When the Auto Select Return Transport Tunnel parameter is enabled, 5620 SAM will consider and use a portion of the bandwidth you specified when setting the SDP Admin Bandwidth parameter in step 9.

a Allow the 5620 SAM to configure the transport tunnel automatically by choosing a profile name. See Procedure 27-3 for more information about how to create a service tunnel profile.

i Click on the Return tab.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Click on the Select button beside the Profile Name parameter. The Select Return Tunnel Selection Profile - Spoke SDP Binding form opens.

iv Choose a tunnel selection profile and click on the OK button. The Select Return Tunnel Selection Profile - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the profile name displayed.

b Allow the 5620 SAM to configure the transport tunnel automatically by choosing a transport encapsulation type.

i Click on the Return tab.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Configure the Return Tunnel Auto-Selection Transport Preference parameter.

c Configure the transport tunnel manually.

i Click on the Return tab.

ii Click on the Select button in the Return Tunnel panel. The Select Return Tunnel - Spoke SDP Binding form opens. See Procedure 27-1 for more information about how to create a service tunnel

iii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Return Tunnel - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the service Tunnel ID, Name, and Underlying Transport displayed in the Tunnel panel.

11 Click on Select in the Return SDP Binding Endpoint panel to choose a Return Endpoint on the terminating site. Select the required endpoint from the drop-down list that appears.

12 Click on the States tab.

13 Configure the Administrative State parameter.

14 Click on the Pseudowire OAM tab.

15 Configure the Control Word parameter.

If you set the VC Type parameter to FR-DLCI in step 4 of Procedure 67-12, you must set the Control Word parameter to Preferred.

16 Assign ingress and egress ACL filters to the spoke SDP binding, if required.

i Click on the ACL tab.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - Spoke SDP Binding form opens.

iii Choose an ingress ACL filter and click on the OK button. The Select Ingress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding form reappears with the ingress ACL filter information displayed.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - Spoke SDP Binding form opens.

v Choose an egress ACL filter and click on the OK button. The Select Egress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding form reappears with the egress ACL filter information displayed.

17 Click on the OK button. The Spoke SDP Binding (Create) form closes and a dialog box appears.

18 Click on the OK button. The Fpipe Site (Create) form reappears with the new information displayed in the service navigation tree.

19 Click on the OK button. The Fpipe Site (Edit) form closes and a dialog box appears.

20 Click on the OK button. The Fpipe Service (Edit) form reappears with the new information displayed in the service navigation tree.

21 Close the Fpipe Service (Edit) form.

Procedure 67-15 To create a VLL Hpipe service

VLL Hpipe services are configurable only on the 7705 SAR and 7705 SAR-M, Release 5.0 and later.

In order to configure a VLL Hpipe service on a supporting NE, the daughter card MDA Mode must be set to cem-fr-hdlc-ppp. For more information, see Procedure 15-33. Only ports that are configured with an Encap Type of HDLC can be mapped to an Hpipe SAP. For more information, see Procedure 16-1.

1 Choose Create→Service→VLL→Hpipe (HDLC to HDLC) from the 5620 SAM main menu. The Hpipe Service (Create) form opens.

2 Click on the Select button to choose a customer to associate with the VLL Hpipe service. The Select Customer - Hpipe Service form opens.

3 Choose a customer for the VLL Hpipe service and click on the OK button. The Select Customer - Hpipe Service form closes and the Hpipe Service (Create) form refreshes with the customer information displayed.

4 Configure the parameters:

- Service ID
- Auto-Assign ID
- SVC Mgr Service ID
- Default VC ID
- Inherit Service ID Value
- Service Name
- Description
- Service Tier
- Service Priority
- Administrative State
- VC Type
- Automatic SDP Binding/PBB Tunnel Creation

The Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.

The SVC Mgr Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.

The Default VC ID parameter is configurable when the Inherit Service ID Value parameter is disabled.

5 Configure the OLC state:

i Click on the Apply button.

ii Configure the parameters:

- Current OLC State
- Revert OLC State

6 If you enabled the Automatic SDP Binding/PBB Tunnel Creation parameter in step 4, perform the following steps. Otherwise, go to step 7.

i Click on the Select button beside the Profile Name parameter. The Select Tunnel Selection Profile - Hpipe Service - Subscriber form opens.

ii Choose a tunnel selection profile from the list and click on the OK button. The Select Tunnel Selection Profile - Hpipe Service - Subscriber form closes and the Hpipe Service (Create) form refreshes with the tunnel selection profile information.

iii Configure the Transport Type parameter. The Transport Type parameter is configurable only when the Profile Name parameter is not configured.

7 To configure service tunnel required bandwidth for the service, perform the following steps.



Note — In order to configure service tunnel required bandwidth, you must enable multi-segment tunnel selection and service bandwidth management at the system level. For more information see the *5620 SAM System Administrator Guide*.

i Click on the Bandwidth tab.

ii Configure the Bandwidth Method parameter.

iii If the Bandwidth Method parameter is set to Input Manually or Calculate from SAPs, configure LSP Path Booking and Service Path Booking parameters.

iv If the Bandwidth Method parameter is set to Input Manually, enter a required bandwidth value for each CoS (see CoS 0 Bandwidth - CoS 7 Bandwidth).

8 Click on the OK button. A dialog box appears.

9 Click on the OK button. The Hpipe Service (Create) form closes.

You can use the service topology maps to view the service. See chapter 6 for more information about service topology maps.

10 To create a site for the Hpipe, perform Procedure 67-16.

For information on adding a GNE site to a VLL service, see Procedure 67-25.

Procedure 67-16 To create a VLL Hpipe site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VLL service and click on the Properties button. The Apipe Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 On the navigation tree, right-click on Hpipe Service and choose Create Hpipe Site. The Select Network Elements - Hpipe form opens with a list of available NEs.

5 Choose a site and click on the OK button. The Hpipe Site (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Name
- Description
- MTU
- MTU Check
- Administrative State
- Monitor Access Interface Operational State
- VLL Site Type

7 To configure service tunnel required bandwidth for the site, perform the following steps.



Note — In order to configure service tunnel required bandwidth, you must enable multi-segment tunnel selection and service bandwidth management at the system level. For more information see the *5620 SAM System Administrator Guide*.

i Click on the Bandwidth tab.

ii Enable the Override Service Configuration parameter.

iii Configure the Bandwidth Method parameter.

iv If the Bandwidth Method parameter is set to Input Manually, enter a required bandwidth value for each CoS (see CoS 0 Bandwidth - CoS 7 Bandwidth).

8 Click on the OK button. The Hpipe Site (Create) form closes and a dialog box appears.

9 Click on the OK button. The Hpipe Service (Edit) form reappears with the new information displayed in the service navigation tree.

10 Create an additional site for the VLL service, if required. Repeat steps 4 to 8.

11 Close the Hpipe Service (Edit) form.

12 Perform one of the following:

a Create endpoints for a redundant VLL. Perform Procedure 67-26.

b Create an L2 access interface for the VLL terminating site. Perform Procedure 67-27.

c Create a spoke SDP binding for the site. Perform Procedure 67-17.

Procedure 67-17 To create a spoke SDP binding on a VLL Hpipe site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VLL service and click on the Properties button. The Hpipe Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 On the navigation tree, right-click on Spoke SDP Bindings and choose Create Spoke SDP Binding. The Spoke SDP Binding (Create) form opens with the General tab displayed.

5 Specify a destination NE for the spoke SDP binding:

a If the destination NE is a managed NE, choose from a list of managed NEs.

i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element - Spoke SDP Binding form opens.

ii Choose a destination NE and click on the OK button. The Select Destination Network Element - Spoke SDP Binding (Create) form closes and the Spoke SDP Binding form refreshes with the tunnel termination site (the destination NE) identifier displayed.

b If the destination NE is an unmanaged NE, specify the system ID for the Tunnel Termination Site parameter.

6 Configure the parameters:

- VC ID
- Auto-Assign ID
- Ingress Label
- Egress Label

The VC IDparameter is configurable when the Auto-Assign ID parameter is disabled.

7 Perform one of the following to specify a transport tunnel for the spoke SDP binding.

a Allow the 5620 SAM to configure the transport tunnel automatically by choosing a profile name. See Procedure 27-3 for more information about how to create a service tunnel profile.

i Enable the Auto-Select Transport Tunnel parameter.

ii Click on the Select button beside the Profile Name parameter. The Select Tunnel Selection Profile - Spoke SDP Binding form opens.

iii Choose a tunnel selection profile and click on the OK button. The Select Tunnel Selection Profile - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the profile name displayed.

b Allow the 5620 SAM to configure the transport tunnel automatically by choosing a transport encapsulation type.

i Enable the Auto-Select Transport Tunnel parameter.

ii Configure the Tunnel Auto-Selection Transport Preference parameter.

c Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens. See Procedure 27-1 for more information about how to create a service tunnel.

ii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier.



Note — The 5620 SAM blocks the manual selection of a tunnel with insufficient bandwidth if the server configuration includes the following parameter setting:

<vll-CAC enforceTunnelBandwidth="true"/>

The parameter is set to false by default, which means that the 5620 SAM does not block the manual selection of a tunnel with insufficient bandwidth; instead, the “Insufficient Bandwidth To Allocate To SDP Binding” State Cause indicator is set.

To change the parameter setting, contact Alcatel-Lucent technical support.

8 If you are creating redundant SDP bindings, configure the endpoint in the Redundancy panel:

i Click on the Select button in the Redundancy panel to select an endpoint for the transport tunnel. The drop-down menu displays the available endpoints.

ii Configure the parameters:

- Precedence
- Active State

9 Perform one of the following to specify a transport tunnel for the Return SDP binding, if required.



Note 1 — You can create a return tunnel only between sites that are in the same service. If the sites are not in the same service, the Return tab does not appear.

Note 2 — When the Auto Select Return Transport Tunnel parameter is enabled, 5620 SAM will consider and use a portion of the bandwidth you specified when setting the SDP Admin Bandwidth parameter in step 10.

a Allow the 5620 SAM to configure the transport tunnel automatically by choosing a profile name. See Procedure 27-3 for more information about how to create a service tunnel profile.

i Click on the Return tab.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Click on the Select button beside the Profile Name parameter. The Select Return Tunnel Selection Profile - Spoke SDP Binding form opens.

iv Choose a tunnel selection profile and click on the OK button. The Select Return Tunnel Selection Profile - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the profile name displayed.

b Allow the 5620 SAM to configure the transport tunnel automatically by choosing a transport encapsulation type.

i Click on the Return tab.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Configure the Return Tunnel Auto-Selection Transport Preference parameter.

c Configure the transport tunnel manually.

i Click on the Return tab.

ii Click on the Select button in the Return Tunnel panel. The Select Return Tunnel - Spoke SDP Binding form opens. See Procedure 27-1 for more information about how to create a service tunnel

iii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Return Tunnel - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the service Tunnel ID, Name, and Underlying Transport displayed in the Tunnel panel.

10 Click on Select in the Return SDP Binding Endpoint panel to choose a Return Endpoint on the terminating site. Select the required endpoint from the drop-down list that appears.

11 Click on the States tab.

12 Configure the Administrative State parameter.

13 Click on the Pseudowire OAM tab.

14 Configure the Control Word parameter.

If you set the VC Type parameter to HDLC in step 4 of Procedure 67-12, you must set the Control Word parameter to Preferred.

15 Click on the OK button. The Spoke SDP Binding (Create) form closes and a dialog box appears.

16 Click on the OK button. The Hpipe Site (Edit) form reappears with the spoke SDP binding displayed in the service navigation tree.

17 Close the Hpipe Service (Edit) form.

Procedure 67-18 To create a VLL Ipipe service

1 Choose Create→Service→VLL→Ipipe from the 5620 SAM main menu. The Ipipe Service (Create) form opens.

2 Click on the Select button to choose a customer to associate with the VLL service. The Select Customer - Ipipe Service form opens.

3 Choose a customer for the VLL service and click on the OK button. The Select Customer - Ipipe Service form closes and the Ipipe Service (Create) form refreshes with the customer information displayed.

4 Configure the parameters:

- Service ID
- Auto-Assign ID
- SVC Mgr Service ID
- Default VC ID
- Inherit Service ID Value
- Service Name
- Description
- Service Tier
- Service Priority
- Administrative State
- Automatic SDP Binding/PBB Tunnel Creation

The Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.

The SVC Mgr Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.

The Default VC ID parameter is configurable when the Inherit Service ID Value parameter is disabled.

5 Configure the OLC state:

i Click on the Apply button.

ii Configure the parameters:

- Current OLC State
- Revert OLC State

6 If you enabled the Automatic SDP Binding/PBB Tunnel Creation parameter in step 4, perform the following steps. Otherwise, go to step 7.

i Click on the Select button beside the Profile Name parameter. The Select Tunnel Selection Profile - Ipipe Service - Subscriber form opens.

ii Choose a tunnel selection profile from the list and click on the OK button. The Select Tunnel Selection Profile - Ipipe Service - Subscriber form closes and the Ipipe Service (Create) form refreshes with the tunnel selection profile information.

iii Configure the Transport Type parameter. The Transport Type parameter is configurable only when the Profile Name parameter is not configured.

7 To configure parameters for AA reporting to the 5670 RAM, perform the following steps.

i Click on the Application Assurance tab. The 5670 RAM Parameters tab is displayed.

ii Configure the parameters:

- Enable Application Performance Reporting
- Report Customer Name
- Number of IP Detail Addresses

iii To configure one or more custom DCP groups, see the custom DCP group configuration procedure in chapter 76.

iv To specify an application or application group for IP detail reporting, click on the IP Detail Application or IP Detail Application Group tab, as required. The IP Detail Application or IP Detail Application Group (Create) form opens.

Otherwise, go to step 8.

v Configure the parameters:

- ID
- Auto-Assign ID

vi Click on the Select button and choose an application or application group from the Select Application or Select Application Group form.

vii Click on the OK button. The IP Detail Application or IP Detail Application Group (Create) form closes, and a dialog box appears.

viii Click on the OK button. The application or application group is listed on the Ipipe Service (Create) form.

ix To specify another application or application group for IP detail reporting, repeat steps 7 iv to viii.



Note — You can specify up to 10 applications and up to 10 application groups.

8 To configure service tunnel required bandwidth for the service, perform the following steps.



Note — In order to configure service tunnel required bandwidth, you must enable multi-segment tunnel selection and service bandwidth management at the system level. For more information see the *5620 SAM System Administrator Guide*.

i Click on the Bandwidth tab.

ii Configure the Bandwidth Method parameter.

iii If the Bandwidth Method parameter is set to Input Manually or Calculate from SAPs, configure LSP Path Booking and Service Path Booking parameters.

iv If the Bandwidth Method parameter is set to Input Manually, enter a required bandwidth value for each CoS (see CoS 0 Bandwidth - CoS 7 Bandwidth).

9 Click on the OK button. The Ipipe Service (Create) form reappears.

10 Click on the OK button. The Ipipe Service (Create) form closes.

You can use the service topology maps to view the service. See chapter 6 for more information about service topology maps.

11 To create a site for the VLL, perform Procedure 67-19.

For information on adding a GNE site to a VLL service, see Procedure 67-25.

Procedure 67-19 To create a VLL Ipipe site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VLL service and click on the Properties button. The Ipipe Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 On the navigation tree, right-click on Ipipe Service and choose Create Ipipe Site. The Select Network Elements - Ipipe Service form opens with a list of available NEs.

5 Choose a site and click on the OK button. The Ipipe Site (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Name
- Description
- MTU
- Administrative State
- Monitor Access Interface Operational State
- Enable CE IP Address Discovery
- Stack Capability Signaling
- Tunnel Fault Notification

The Enable CE IP Address Discovery parameter is configurable only for VLL terminating sites.

The Stack Capability Signaling parameter is configurable only when the Enable IPv6 parameter and the Enable CE IP Address Discover parameters are enabled.

The Tunnel Fault Notification parameter is configurable on sites where the device has ports configured in access or hybrid mode with QinQ encapsulation. If you are configuring a tunnel facility MEP, this parameter must be set to Accept, in order to accept the fault notification from the tunnel facility MEP.

7 Configure the NE-specific parameters, as shown in Table 67-9.

Table 67-9 NE-specific parameters

NE	Parameters	Dependencies
7450 ESS, 7750 SR, 7705 SAR, and 7950 XRS	VLL Site Type	No dependencies
7450 ESS in mixed mode (chassis mode D and above), 7710 SR (chassis mode C and above), and 7750 SR (chassis mode C, and chassis modes A and B with mixed mode enabled)	Enable IPv6	The Enable CE IP Address Discovery parameter must be enabled.

8 To configure service tunnel required bandwidth for the site, perform the following steps.



Note — In order to configure service tunnel required bandwidth, you must enable multi-segment tunnel selection and service bandwidth management at the system level. For more information see the *5620 SAM System Administrator Guide*.

i Click on the Bandwidth tab.

ii Enable the Override Service Configuration parameter.

iii Configure the Bandwidth Method parameter.

iv If the Bandwidth Method parameter is set to Input Manually, enter a required bandwidth value for each CoS (see CoS 0 Bandwidth - CoS 7 Bandwidth).

9 Click on the OK button. The Ipipe Site (Create) form closes.

10 Create an additional site for the VLL service, if required. Repeat steps 4 to 9.

11 Perform one of the following:

a Create endpoints for a redundant VLL. Perform Procedure 67-26.



Note — Redundant VLL Ipipe services are configurable only on the 7705 SAR, 7450 ESS, 7710 SR, and 7750 SR.

b Create an L2 access interface for the VLL terminating site. Perform Procedure 67-27.

c Create a spoke SDP binding for the site. Perform Procedure 67-20.

Procedure 67-20 To create a spoke SDP binding on a VLL Ipipe site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VLL service and click on the Properties button. The Ipipe Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 On the navigation tree, right-click on Spoke SDP Bindings and choose Create Spoke SDP Binding. The Spoke SDP Binding (Create) form opens with the General tab displayed.

5 Specify a destination NE for the spoke SDP binding:

a If the destination NE is a managed NE, choose from a list of managed NEs.

i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element - Spoke SDP Binding form opens.

ii Choose a destination NE and click on the OK button. The Select Destination Network Element - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the tunnel termination site (the destination NE) identifier displayed.

b If the destination NE is an unmanaged NE, specify the system ID for the Tunnel Termination Site parameter.

6 Configure the parameters:

- Description
- Auto-Assign ID
- VC ID
- Ingress Label
- Egress Label

The VC ID parameter is configurable when the Auto-Assign ID parameter is disabled.

7 Perform one of the following to specify a transport tunnel for the spoke SDP binding.

a Allow the 5620 SAM to configure the transport tunnel automatically by choosing a profile name. See Procedure 27-3 for more information about how to create a service tunnel profile.

i Enable the Auto-Select Transport Tunnel parameter.

ii Click on the Select button beside the Profile Name parameter. The Select Tunnel Selection Profile - Spoke SDP Binding form opens.

iii Choose a tunnel selection profile and click on the OK button. The Select Tunnel Selection Profile - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the profile name displayed.

b Allow the 5620 SAM to configure the transport tunnel automatically by choosing a transport encapsulation type.

i Enable the Auto-Select Transport Tunnel parameter.

ii Configure the Tunnel Auto-Selection Transport Preference parameter.

c Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens. See Procedure 27-1 for more information about how to create a service tunnel.

ii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier.



Note — The 5620 SAM blocks the manual selection of a tunnel with insufficient bandwidth if the server configuration includes the following parameter setting:

<vll-CAC enforceTunnelBandwidth="true"/>

The parameter is set to false by default, which means that the 5620 SAM does not block the manual selection of a tunnel with insufficient bandwidth; instead, the “Insufficient Bandwidth To Allocate To SDP Binding” State Cause indicator is set.

To change the parameter setting, contact Alcatel-Lucent technical support.

8 If you are creating redundant SDP bindings, configure the endpoint in the Redundancy panel:

i Click on the Select button in the Redundancy panel to select an endpoint for the transport tunnel. The drop-down menu displays the available endpoints.

ii Configure the parameters:

- Inter-Chassis Backup
- Precedence
- Active State

9 Configure the parameters:

- Enable Hash Label
- Enable Signal Capability
- SDP Admin Bandwidth

10 Perform one of the following to specify a transport tunnel for the Return SDP binding, if required.



Note 1 — You can create a return tunnel only between sites that are in the same service. If the sites are not in the same service, the Return tab does not appear.

Note 2 — When the Auto Select Return Transport Tunnel parameter is enabled, 5620 SAM will consider and use a portion of the bandwidth you specified when setting the SDP Admin Bandwidth parameter in step 9.

a Allow the 5620 SAM to configure the transport tunnel automatically by choosing a profile name. See Procedure 27-3 for more information about how to create a service tunnel profile.

i Click on the Return tab.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Click on the Select button beside the Profile Name parameter. The Select Return Tunnel Selection Profile - Spoke SDP Binding form opens.

iv Choose a tunnel selection profile and click on the OK button. The Select Return Tunnel Selection Profile - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the profile name displayed.

b Allow the 5620 SAM to configure the transport tunnel automatically by choosing a transport encapsulation type.

i Click on the Return tab.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Configure the Return Tunnel Auto-Selection Transport Preference parameter.

c Configure the transport tunnel manually.

i Click on the Return tab.

ii Click on the Select button in the Return Tunnel panel. The Select Return Tunnel - Spoke SDP Binding form opens. See Procedure 27-1 for more information about how to create a service tunnel

iii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Return Tunnel - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the service Tunnel ID, Name, and Underlying Transport displayed in the Tunnel panel.

11 Click on Select in the Return SDP Binding Endpoint panel to choose a Return Endpoint on the terminating site. Select the required endpoint from the drop-down list that appears.

12 Choose an Application Profile for the spoke SDP binding.

i Click on the Select button beside the Application Profile parameter. The Application Profile String: - Spoke SDP Binding form opens. See Procedure 76-1 for more information about how to configure an application profile.

ii Configure the filter criteria. A list of Application Profiles appears.

iii Choose an application profile from the list and click on the OK button. The Application Profile String: - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form appears.



Note — The Application Profile String: - Spoke SDP Binding service form displays only local profiles on the NE.

13 Associate an AA transit prefix policy with the service object, if required. See Procedure 76-10 for more information about how to configure a transit prefix policy.

i Click on the Select button in the Transit Prefix Policy panel. The Select Transit Prefix Policy form opens.

ii Select a transit IP policy and click on the OK button.

14 To configure custom object attributes for AA reporting to the 5670 RAM, perform the following steps:

i Click on the 5670 RAM Parameters tab.

ii Click on the Reporting tab.

iii Click on the Create button. The AA Reporting (Create) form opens.

iv Configure the parameters:

- Customer Name
- Subscriber Name
- Subscriber Class
- Subscriber Type
- Total Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 1 Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 2 Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 3 Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 4 Bandwidth Upstream (Kbps)
- Downstream (Kbps)

v Click on the OK button. The AA Reporting (Create) form closes and the reporting object is displayed in the list.

vi Click on the General tab.

15 Click on the QoS tab.

16 Configure the required parameters in the Forwarding Plane Redirect panel:

i Click on the Network Policy Select button to assign a policy to the Spoke SDP Binding. The Select Network Policy form opens.

ii Choose a policy from the list and click on the OK button. The Network Policy form closes.

iii Click on the Ingress Queue Group Template Policy Select button to assign a policy to the Spoke SDP Binding. The Select Ingress Queue Group Template Policy form opens.

iv Choose a policy from the list and click on the OK button. The Ingress Queue Group Template Policy form closes.

v Configure the Instance ID parameter.



Note — The Network Policy, Ingress Queue Group Template Policy and the Instance ID parameter must be configured if you modify any of the parameters on the Forwarding Plane Redirect panel.

17 Configure the required parameters in the Port Redirect panel:

i Click on the Network Policy Select button to assign a policy to the Spoke SDP Binding. The Select Network Policy form opens.

ii Choose a policy from the list and click on the OK button. The Network Policy form closes.

iii Click on the Egress Queue Group Template Policy Select button to assign a policy to the Spoke SDP Binding. The Select Egress Queue Group Template Policy form opens.

iv Choose a policy from the list and click on the OK button. The Egress Queue Group Template Policy form closes.

v Configure the Instance ID parameter.

18 Click on the States tab.

19 Configure the Administrative State parameter.

20 Click on the Pseudowire OAM tab.

21 Configure the Control Word parameter.

22 Assign ingress and egress ACL filters to the spoke SDP binding, if required. See chapter 44 for more information about how to configure filter policies.

i Click on the ACL tab.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - Spoke SDP Binding form opens.

iii Choose an ingress ACL filter and click on the OK button. The Select Ingress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding form reappears with the ingress ACL filter information displayed.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - Spoke SDP Binding form opens.

v Choose an egress ACL filter and click on the OK button. The Select Egress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding form reappears with the egress ACL filter information displayed.

vi Click on the Select button in the IPv6 Ingress Filter panel to choose an IPv6 ingress ACL filter. The Select IPv6 Ingress Filter - Spoke SDP Binding form opens.

vii Choose an IPv6 ingress filter and click on the OK button. The Select IPv6 Ingress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding form reappears with the IPv6 ingress ACL filter information displayed.

viii Click on the Select button in the IPv6 Egress Filter panel to choose an IPv6 egress ACL filter. The Select IPv6 Egress Filter - Spoke SDP Binding form opens.

ix Choose an IPv6 egress filter and click on the OK button. The Select IPv6 Egress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding form reappears with the IPv6 egress ACL filter information displayed.

23 Click on the Ipipe tab.

24 Configure the Peer CE IP Address parameter.

25 Click on the OK button. The Spoke SDP Binding (Edit) form closes and a dialog box appears.

26 Click on the OK button. The Ipipe Site (Edit) form reappears with the spoke SDP binding displayed in the service navigation tree.

27 Close the Ipipe Service (Edit) form.

Procedure 67-21 To create a VLL Cpipe service

VLL Cpipe services are configurable only on the 7710 SR, 7750 SR, 7705 SAR, 7210 SAS-M, and 7450 ESS devices. Consider the following when creating a VLL Cpipe:

- The Time Slots parameter of the DS0 channel must be configured with at least one time slot.
- Time slots are automatically configured for unstructured E1 and T1 endpoints
- The Clock Source parameter of the DS1 channel must be set to Node-Timed.

1 Choose Create→Service→VLL→Cpipe (CEM to CEM) from the 5620 SAM main menu. The Cpipe Service (Create) form opens.

2 Click on the Select button to choose a customer to associate with the VLL service. The Select Customer - Cpipe Service form opens.

3 Choose a customer for the VLL service and click on the OK button. The Select Customer - Cpipe Service form closes and the Cpipe Service (Create) form refreshes with the customer information displayed. See Procedure 64-1 for information about how to create a customer.

4 Configure the parameters:

- Service ID
- Auto-Assign ID
- SVC Mgr Service ID
- Default VC ID
- Inherit Service ID Value
- Service Name
- Description
- Service Tier
- Service Priority
- Administrative State
- VC Type
- Automatic SDP Binding/PBB Tunnel Creation
- Use Bandwidth-Reserved Paths

The Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.

The SVC Mgr Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.

The Default VC ID parameter is configurable when the Inherit Service ID Value parameter is disabled.

5 Configure the OLC state:

i Click on the Apply button.

ii Configure the parameters:

- Current OLC State
- Revert OLC State

6 If you enabled the Automatic SDP Binding/PBB Tunnel Creation parameter in step 4, perform the following steps. Otherwise, go to step 7.

i Click on the Select button beside the Profile Name parameter. The Select Tunnel Selection Profile - Cpipe Service - Subscriber form opens.

ii Choose a tunnel selection profile from the list and click on the OK button. The Select Tunnel Selection Profile - Cpipe Service - Subscriber form closes and the Cpipe Service (Create) form refreshes with the tunnel selection profile information.

iii Configure the Transport Type parameter. The Transport Type parameter is configurable only when the Profile Name parameter is not configured.

7 To configure service tunnel required bandwidth for the service, perform the following steps.



Note — In order to configure service tunnel required bandwidth, you must enable multi-segment tunnel selection and service bandwidth management at the system level. For more information see the *5620 SAM System Administrator Guide*.

i Click on the Bandwidth tab.

ii Configure the Bandwidth Method parameter.

iii If the Bandwidth Method parameter is set to Input Manually or Calculate from SAPs, configure LSP Path Booking and Service Path Booking parameters.

iv If the Bandwidth Method parameter is set to Input Manually, enter a required bandwidth value for each CoS (see CoS 0 Bandwidth - CoS 7 Bandwidth).

8 Perform one of the following:

a Create a site for the VLL. Go to step 4.

b Complete VLL creation if sites and interfaces are to be created later. Go to step 9.

For information on adding a GNE site to a VLL service, see Procedure 67-25.

9 Click on the OK button. The Cpipe Service (Create) form closes.

You can use the service topology maps to view the service. See chapter 6 for more information about service topology maps.

Procedure 67-22 To create a VLL Cpipe site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VLL service and click on the Properties button. The Cpipe Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 On the navigation tree, right-click on Cpipe Service and choose Create Cpipe Site. The Select Network Elements - Cpipe Service form opens with a list of available NEs.

5 Choose a site and click on the OK button. The Select Network Elements - Cpipe Service form closes and the Cpipe Site (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Name
- Description
- MTU
- Administrative State
- Monitor Access Interface Operational State
- VLL Site Type

7 To configure service tunnel required bandwidth for the site, perform the following steps.



Note — In order to configure service tunnel required bandwidth, you must enable multi-segment tunnel selection and service bandwidth management at the system level. For more information see the *5620 SAM System Administrator Guide*.

i Click on the Bandwidth tab.

ii Enable the Override Service Configuration parameter.

iii Configure the Bandwidth Method parameter.

iv If the Bandwidth Method parameter is set to Input Manually, enter a required bandwidth value for each CoS (see CoS 0 Bandwidth - CoS 7 Bandwidth).

8 Click on the OK button. The Site (Create) form closes and a dialog box appears.

9 Click on the OK button. The Cpipe Service (Edit) form reappears with the new information displayed in the service navigation tree.

10 Create an additional site for the VLL service, if required. Repeat steps 4 to 9.

11 Perform one of the following:

a Create endpoints for a redundant VLL. Perform Procedure 67-26.

b Create an L2 access interface for the VLL terminating site. Perform Procedure 67-27.

c Create a spoke SDP binding for the site. Perform Procedure 67-23.

Procedure 67-23 To create a spoke SDP binding on a VLL Cpipe site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VLL service and click on the Properties button. The Cpipe Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 On the navigation tree, right-click on Spoke SDP Bindings and choose Create Spoke SDP Binding. The Spoke SDP Binding (Create) form opens with the General tab displayed.

5 Specify a destination NE for the spoke SDP binding:

a If the destination NE is a managed NE, choose from a list of managed NEs.

i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element - Spoke SDP Binding form opens.

ii Choose a destination NE and click on the OK button. The Select Destination Network Element - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the tunnel termination site (the destination NE) identifier displayed.

b If the destination NE is an unmanaged NE, specify the system ID for the Tunnel Termination Site parameter.

6 Configure the parameters:

- Auto-Assign ID
- VC ID
- Ingress Label
- Egress Label
- SDP Admin Bandwidth

The VC ID parameter is configurable when the Auto-Assign ID parameter is disabled.



Note — The SDP Admin Bandwidth parameter is not configurable if you select an MPLS-TP tunnel in step 7.

7 Perform one of the following to specify a transport tunnel for the spoke SDP binding.

a Allow the 5620 SAM to configure the transport tunnel automatically by choosing a profile name. See Procedure 27-3 for more information about how to create a service tunnel profile.

i Enable the Auto-Select Transport Tunnel parameter.

ii Click on the Select button beside the Profile Name parameter. The Select Tunnel Selection Profile - Spoke SDP Binding form opens.

iii Choose a tunnel selection profile and click on the OK button. The Select Tunnel Selection Profile - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the profile name displayed.

b Allow the 5620 SAM to configure the transport tunnel automatically by choosing a transport encapsulation type.

i Enable the Auto-Select Transport Tunnel parameter.

ii Configure the Tunnel Auto-Selection Transport Preference parameter.

c Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens. See Procedure 27-1 for more information about how to create a service tunnel.

ii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier.



Note — The 5620 SAM blocks the manual selection of a tunnel with insufficient bandwidth if the server configuration includes the following parameter setting:

<vll-CAC enforceTunnelBandwidth="true"/>

The parameter is set to false by default, which means that the 5620 SAM does not block the manual selection of a tunnel with insufficient bandwidth; instead, the “Insufficient Bandwidth To Allocate To SDP Binding” State Cause indicator is set.

To change the parameter setting, contact Alcatel-Lucent technical support.

d Configure an MPLS-TP transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens.

ii Select an MPLS-TP service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier. See Procedure 27-1 for more information about how to create an MPLS-TP service tunnel.

8 If you are creating redundant SDP bindings, configure the endpoint in the Redundancy panel:

i Click on the Select button in the Redundancy panel to select an endpoint for the transport tunnel. The drop-down menu displays the available endpoints.

ii Configure the parameters:

- Inter-Chassis Backup
- Precedence
- Active State

9 Perform one of the following to specify a transport tunnel for the Return SDP binding, if required.



Note 1 — You can create a return tunnel only between sites that are in the same service. If the sites are not in the same service, the Return tab does not appear.

Note 2 — When the Auto Select Return Transport Tunnel parameter is enabled, 5620 SAM will consider and use a portion of the bandwidth you specified when setting the SDP Admin Bandwidth parameter in step 6.

a Allow the 5620 SAM to configure the transport tunnel automatically by choosing a profile name. See Procedure 27-3 for more information about how to create a service tunnel profile.

i Click on the Return tab.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Click on the Select button beside the Profile Name parameter. The Select Return Tunnel Selection Profile - Spoke SDP Binding form opens.

iv Choose a tunnel selection profile and click on the OK button. The Select Return Tunnel Selection Profile - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the profile name displayed.

b Allow the 5620 SAM to configure the transport tunnel automatically by choosing a transport encapsulation type.

i Click on the Return tab.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Configure the Return Tunnel Auto-Selection Transport Preference parameter.

c Configure the transport tunnel manually.

i Click on the Return tab.

ii Click on the Select button in the Return Tunnel panel. The Select Return Tunnel - Spoke SDP Binding form opens. See Procedure 27-1 for more information about how to create a service tunnel

iii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Return Tunnel - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the service Tunnel ID, Name, and Underlying Transport displayed in the Tunnel panel.

10 Click on Select in the Return SDP Binding Endpoint panel to choose a Return Endpoint on the terminating site. Select the required endpoint from the drop-down list that appears.

11 Click on the States tab.

12 Configure the Administrative State parameter.

13 Click on the Pseudowire OAM tab.

14 Configure the Control Word parameter.

15 Click on the OK button. The Spoke SDP Binding (Create) form closes and a dialog box appears.

16 Click on the OK button. The Site (Edit) form reappears with the new spoke SDP binding information displayed in the service navigation tree.

17 Close the Site (Edit) form.

Procedure 67-24 To configure an MPLS-TP static pseudowire on an Cpipe spoke SDP binding

Perform this procedure to create an MPLS-TP static pseudowire on the spoke SDP binding. An MPLS-TP service tunnel must be used in the SDP binding, and the Control Word parameter for pseudowire OAM must be set to Preferred. See Procedure 67-23.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Select a Cpipe and click on the Properties button. The Cpipe Service (Edit) form opens.

4 On the navigation tree, expand the site on which you want to configure the spoke SDP binding, and expand the Spoke SDP Bindings icon.

5 Click on the SDP binding on which you want to configure the MPLS-TP static pseudowire. The Spoke SDP Binding (Edit) form opens with the General tab displayed.

6 Click on the Control Channel tab.

7 Configure the parameters:

- Status
- Refresh Timer (seconds)
- Request Timer (seconds)
- Retry Timer (seconds)
- Timeout Multiplier
- Acknowledged

8 Click on the MPLS-TP PW tab.

9 Click on the Create button. The PW Path ID (Create) form opens.

10 Configure the Path AGI parameter.

11 Configure the parameters in the Source Attachment Individual Identifier panel:

- SAII Global ID
- SAII Node ID
- SAII AC ID

12 Configure the parameters in the Target Attachment Individual Identifier panel:

- TAII Global ID
- TAII Node ID
- TAII AC ID

13 Click on the OK button. The PW Path ID (Create) form closes.

14 Click on the OK button. The Spoke SDP Binding (Edit) form closes.

15 Close the Cpipe Service (Edit) form.

16 Close the Manage Services form.

Procedure 67-25 To configure a GNE site on a VLL service

Use this procedure to add a GNE site and GNE service interfaces to an existing VLL service. This procedure applies to VLL Epipe, Apipe, Fpipe, Ipipe, and Cpipe services. This procedure also applies to 9500 MPR VLL Epipe, Apipe, and Cpipe services.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a VLL service and click on the Properties button. The *VLL_type* Service (Edit) form opens with the General tab displayed.

4 On the component tree, right-click on *VLL_type* Service and choose Create GNE Site. The Select Network Elements - *VLL_type* Service form opens with a list of available NEs.

5 Choose a site and click on the OK button. The GNE Site (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Name
- Description

7 Click on the Apply button.

8 To configure an interface for the GNE site, perform the following steps:

i Click on the GNE Service Interfaces tab and then click on the Create button. The GNE Service Interface (Create) form opens with the general tab displayed.

ii Configure the parameters:

- Name
- Description
- Type

iii Click on the Ports tab and then click on the Select button beside the Interface Index field. The Select Generic NE Interface form appears.

iv Select an interface from the list and click on the OK button. The GNE Service Interface (Create) form reappears with the interface information displayed.

v Configure the parameters:

- Encapsulation Type
- Outer Encapsulation Value
- Inner Encapsulation Value

vi Click on the OK button. The GNE Site (Create) form reappears with the interface information displayed in the service component tree.

9 Click on the Scripts tab to attach or execute configuration scripts on the GNE site.

The Scripts tab displays the script instances and versions that are applied to the device. See the *5620 SAM Scripts and Templates Developer Guide* for more information.

10 Click on the OK button. The *VLL_type* Service (Edit) form reappears with the new information displayed in the service component tree.

11 Click on the OK button. The *VLL_type* Service (Edit) form closes.

You can use the topology maps to view the service. See chapter 6 for more information about service topology maps.

Procedure 67-26 To create an endpoint for a redundant VLL service

To create an endpoint for a redundant VLL service, perform the following procedure.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VLL service and click on the Properties button. The *VLL_type* Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 On the navigation tree, expand the site object, right-click on Endpoints and choose Create Endpoint. The Endpoint (Create) form opens.

5 Perform one of the following.

a If you are creating an endpoint on a VLL Epipe or Hpipe, configure the parameters:

- Name
- Description
- Revert Time (seconds)
- Active Hold Delay (100s of milliseconds)
- Enable PW Standby Signaling Master
- Enable PW Standby Signaling Slave

b If you are creating an endpoint on a VLL Apipe, Fpipe, Ipipe, or Cpipe, configure the parameters:

- Name
- Description
- Revert Time (seconds)
- Active Hold Delay (100s of milliseconds)

6 Click on the OK button. The Endpoint (Create) form closes and a dialog box appears.

7 Click on the OK button. The endpoint object is added to the navigation tree and an Endpoint tab is added to the *VLL_type* Service (Edit) form.

8 Repeat steps 4 to 7 to create additional endpoints in the VLL service.

9 Close the *VLL_type* Service (Edit) form.

Procedure 67-27 To create a VLL L2 access interface on a terminating site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VLL and click on the Properties button. The *VLL_type* Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the entries for the site where you want to create a VLL L2 access interface.

For information on adding a GNE service interface to a VLL service, see Procedure 67-25.

5 Right-click on L2 Access Interfaces and choose Create L2 Access Interface. The L2 Access Interface (Create) form opens with the General tab displayed.



Note — If 7210 SAS-D ETR or 7210 SAS-E sites are connected in a ring network, you must configure an Uplink SAP between the sites.

6 Configure the parameters:

- Description
- Cflowd Type
- Administrative State
- Hold Service Up On SAP Failure
- ATM Connection Type
- MC Ring Node
- Tunnel Fault Notification
- Enable AIS

The ATM Connection Type parameter is configurable only in a VLL Apipe service that has the VC Type parameter set to ATM-cell.

The MC Ring Node and Hold Service Up On SAP Failure parameters are configurable only in a VLL Epipe service.

The Tunnel Fault Notification parameter is configurable on L2 access interfaces where the device has ports configured in access or hybrid mode with QinQ encapsulation. If you are configuring a tunnel facility MEP, this parameter must be set to Accept, in order to receive the fault notification from the tunnel facility MEP.

The Enable AIS parameter is configurable only in a VLL Epipe service where the device has ports configured in access or hybrid mode with QinQ encapsulation to forward AIS frames generated by a tunnel facility MEP.

7 If you are creating a redundant L2 access interface, configure the endpoint in the Redundancy panel:

i Click on the Select button in the Redundancy panel to choose an endpoint for the L2 access interface. The drop-down menu displays the available endpoints.

ii Choose an endpoint from the drop-down menu.

8 Click on the Select button beside the Application Profile parameter. The Application Profile String: - L2 Access Interface form opens.



Note — The Application Profile parameter is configurable only for an Epipe and Ipipe L2 access interface.

9 Choose a profile from the list and click on the OK button. The Application Profile String: - L2 Access Interface form closes and the L2 Access Interface (Create) form is refreshed with the application profile information.

Note — The Application Profile String: - L2 Access Interface form only displays local profiles that are on the NE.

10 Associate an AA transit prefix policy with the service object, if required.

i Click on the Select button in the Transit Prefix Policy panel. The Select Transit Prefix Policy form opens.

ii Select a transit IP policy and click on the OK button.

11 To configure custom object attributes for AA reporting to the 5670 RAM, perform the following steps:

i Click on the 5670 RAM Parameters tab.

ii Click on the Reporting tab.

iii Click on the Create button. The AA Reporting (Create) form opens.

iv Configure the parameters:

- Customer Name
- Subscriber Class
- Total Bandwidth Upstream (Kbps)
- Class of Service 1 Bandwidth Upstream (Kbps)
- Class of Service 2 Bandwidth Upstream (Kbps)
- Class of Service 3 Bandwidth Upstream (Kbps)
- Class of Service 4 Bandwidth Upstream (Kbps)
- Subscriber Name
- Subscriber Type
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)

v Click on the OK button. The AA Reporting (Create) form closes and the reporting object is displayed in the list.

vi Click on the General tab.

12 Click on the Port tab.

13 Click on the Select button to choose a port for the L2 access interface. The Select Terminating Port - L2 Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. The port is then listed when you click on the Search button.

14 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - L2 Access Interface form closes, and the L2 Access Interface (Create) form displays the port information.



Note 1 — When you configure a 3-plus-tag Epipe service, you must choose a port with QinQ encapsulation as one endpoint (SAP). When the other endpoint is an L2 access interface, you must choose a port with dot1q or QinQ encapsulation as the other L2 access interface. Both endpoints must be on the same site. See "Epipe (Ethernet VLL)" in section 67.1 for more information. See Procedures 67-2 and 67-4 for additional configuration requirements for a 3-plus-tag Epipe service.

Note 2 — If you choose an Ethernet tunnel endpoint, the Port form is refreshed and an Ethernet Tunnel tab is added.

Note 3 — If you choose a port that is associated with a 7705 SAR MW link, the Port form is refreshed and a Microwave tab appears. See Procedures 15-11 and 15-12 for more information about configuring a 7705 SAR microwave link and MW link member. If you are configuring microwave compression, see Procedure 67-35.

15 Perform one of the following:



Caution — The creation of a SAP that uses the same port and encapsulation values as an existing inactive MSAP fails under the following conditions:

- If you try to use the 5620 SAM to create a SAP, the configuration fails and the 5620 SAM displays an error message.
- If you use a CLI to create a SAP in a service other than the service that contains the MSAP, the configuration succeeds but the MSAP is inactive until the regular SAP is deleted. Although the 5620 SAM displays the SAP and MSAP, the MSAP remains inactive and consumes resources.
- If you use a CLI to create a SAP in the service that contains the MSAP, the SAP creation fails.

Alcatel-Lucent recommends that you delete an inactive MSAP from the 5620 SAM if you need to create a regular SAP on the same port using the same encapsulation values. See Procedure 65-34 for more information about deleting MSAPs.

a If you are creating an Epipe or Ipipe L2 access interface, configure the parameters:

- Outer Encapsulation Value
- Inner Encapsulation Value
- Outer Encapsulation Value (VPI)
- Inner Encapsulation Value (VCI)
- LLF Enabled
- Transit SAP

When the selected port uses dot1q encapsulation, you can enable the Auto-Assign ID check box to have the Outer Encapsulation Value parameter automatically assigned. If you choose this, the system assigns the lowest unused encapsulation value.



Note — You can set the Auto-Assign ID parameter to be the default parameter for dot1q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter in the User Preferences form. Choose Application→ User Preferences from the main menu.

The Inner Encapsulation Value parameter is configurable only when the port encapsulation type is QinQ.

When you configure a 3-plus-tag Epipe service with L2 access interfaces as both endpoints, you must observe the following requirements:

- One endpoint must be a QinQ SAP
- The other endpoint must be a dot1q SAP or a QinQ SAP (a QinQ SAP as the second endpoint is supported from NE release 5.0 R3 or later).
- When the other endpoint is a dot1q SAP, the outer encapsulation value for the dot1q SAP must match the inner encapsulation value of the QinQ SAP that shares the L2 connection.
- When the other endpoint is a QinQ SAP, the inner encapsulation values for both QinQ SAPs on the service must match.

See "Epipe (Ethernet VLL)" in this chapter for more information. See Procedures 67-2 and 67-4 for additional configuration requirements for a 3-plus-tag Epipe service

The Outer Encapsulation Value (VPI) parameter is configurable only when the port encapsulation type is ATM.

The Inner Encapsulation Value (VCI) parameter is configurable only when the port encapsulation type is ATM.

The LLF Enabled parameter is configurable only for Epipe L2 access interfaces on ports with Null encapsulation.

If the port you have chosen is an Ethernet Tunnel Endpoint, you will be able to set the Outer Encapsulation Value to 8191. This automatically enables the Ethernet Tunnel Endpoint Control SAP parameter.

b If you are creating an Epipe and use dot1q or QinQ encapsulation, you can enable ingress VLAN translation, if required. Configure the parameters:

- Translation
- Translation ID

c If you are creating an Epipe and configuring VLAN ranges on a 7210 SAS, perform the following steps:

i Enable the VLAN Range SAP parameter. The Connection Profile panel is displayed.

ii Click on the Select button and choose a VLAN range.



Note — See Procedure 53-2 fore information about how to create a connection profile with a VLAN range.

d If you are creating an Apipe L2 access interface, configure the parameters:

- Outer Encapsulation Value (VPI)
- Inner Encapsulation Value (VCI)
- Encapsulation Value
- Encapsulation Value
- Encapsulation Value
- LLF Enabled
- Connection Profile ID

The Encapsulation Value parameter and the Encapsulation Value parameter are configurable only when the VC Type parameter is set to ATM-cell in step 4 of Procedure 67-8 and the ATM Connection Type parameter is set to PVT in step 6 of this procedure.

The Encapsulation Value parameter is configurable only when the VC Type parameter is set to ATM-VPC in step 4 of Procedure 67-8.

The LLF Enabled parameter is configurable only for SAPs with “Port” ATM Connection Type and on a clear channel under 4 port OC3-STM1 ASAP MDA.

The Connection Profile ID parameter is configurable only when the Signalling VC Type Override parameter is set to ATM-VCC or None. The Connection Profile ID parameter can only be associated with an Apipe when the VC Type parameter is set to ATM-cell.

e If you are creating an Fpipe L2 access interface, configure the Outer Encapsulation Value parameter.

16 To configure port redundancy for a Cpipe or Epipe service, perform the following steps.



Note — Port redundancy is configurable only on a 7705 SAR or 7750 SR.

i Select the Enable Port Redundancy parameter. The Backup Port Information panel is displayed.

ii Configure the Off-Node Protection parameter.

iii If the Off-Node Protection parameter is enabled, use the Select button beside the Redundant Node ID parameter to choose the site that contains the backup port.



Note — The site that you choose must be the same type and release of device as the site that you are configuring.

iv Use the Select button beside the Redundant Port parameter to choose the redundant port.



Note — Only ports with the same encapsulation type as the currently assigned port are listed.

v Configure the following parameters:

- Outer Encapsulation Value
- Inner Encapsulation Value

17 If you are creating a Cpipe L2 access interface, go to step 22.

18 Configure the Ethernet Tunnel Endpoint Control SAP parameter, if required.



Note — Enabling the Ethernet Tunnel Endpoint Control SAP parameter creates the control L2 Access Interface (also known as a Control SAP). It also automatically sets the value of the Outer Encapsulation Value parameter to 8191.

If you are currently creating a same-fate SAP, the Ethernet Tunnel Endpoint Control SAP parameter must not be enabled.

19 If the selected port uses FR encapsulation, configure Frame Relay for the interface.

i Click on the Frame Relay tab.

ii Set the FRF-12 Mode parameter to Enabled.

iii Configure the parameters:

- FRF-12 End-To-End Fragment Threshold
- Scheduling Class
- Fragment Interleave



Note — If a bundle was selected in step 14, only the Scheduling Class parameter is configurable.

The Fragment Interleave parameter is configurable only in a VLL Epipe or Ipipe service.

20 If you need to create an Epipe or Ipipe L2 access interface, specify the queue overrides by clicking on the Override Policy Items tab.

Note — The Override Policy Items tab contains a number of sub-tabs. However, the sub-tabs that are displayed depend on the port type that you have chosen for this interface.

- If you configured a non-HSMDA port, then the Access Ingress Queues, Access Egress Queues, Ingress Policer, and Egress Policer sub-tabs are active.
- If you configured an HSMDA port, then the Access Ingress Queues, Access Egress HSMDA Queues and Ingress Policer sub-tabs are active.

Set the queue overrides, as described in Procedure 43-42.

21 If you are creating an Ipipe L2 access interface, specify Ipipe functionality for the interface. Otherwise, go to step 22.

i Click on the IPIPE tab.

ii Configure the parameters:

- CE IP Address
- MAC Refresh Interval
- MAC Address
- Use Broadcast MAC Address

The MAC Address parameter, MAC Refresh Interval parameter, and Use Broadcast MAC Address parameters are configurable only when the port encapsulation type is dot1q, QinQ, or Null.

22 Click on the OK button. A dialog box appears.

23 Click on the OK button. The L2 Access Interface (Create) form closes, and the Site (Create) form reappears with the new interface information displayed in the service navigation tree.

24 To create another L2 access interface for the site in the VLL service, repeat steps 5 to 23.

Note — If you are configuring access dual-homing with local switching over PBB tunnels, you must configure two L2 access interfaces. The L2 access interfaces must be on LAGs that participate in the MC LAG. See chapter 39 for information about MC LAGs.

25 Close the *VLL_type* Service (Edit) form.

26 Close the Manage Services form.

Procedure 67-28 To assign ingress and egress QoS policies to a VLL L2 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VLL and click on the Properties button. The *VLL_type* Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface and choose Properties. The VLL L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the QoS tab.

8 To configure a 7450 ESS, 7705 SAR, 7710 SR, 7750 SR, or 7950 XRS, perform the following steps. Otherwise, go to step 27.



Note — Items such as policies, schedulers and filters can be applied later to multiple service components at once by selecting and right-clicking the components in the service navigation tree, choosing Properties, and configuring the parameters on the appropriate tab.

9 Configure the Ingress Match QinQ Dot1P parameter.

The Ingress Match QinQ Dot1P parameter is configurable only on Epipe L2 access interfaces. The Ingress Match QinQ Dot1P parameter is not configurable if the port encapsulation type is ATM or FR.

10 Click on the Select button in the Ingress Policy panel to choose an ingress QoS policy. The Select Ingress Policy - L2 Access Interface form opens.

11 Choose an ingress QoS policy and click on the OK button. The Select Ingress Policy - L2 Access Interface form closes and the L2 Access Interface (Create) form reappears with the ingress QoS policy information displayed.



Note — For Epipe and Ipipe VLL L2 access interfaces, if you select an access ingress policy which has a forwarding class mapped to an ingress queue group, you must ensure that the port you are configuring for the Epipe or Ipipe L2 access interface has the access ingress queue group with the same name created on it.

See Procedure 16-1 in chapter 16 for more information about how to configure Ethernet ports. See chapter 42 for more information about queue group template policies.

12 Click on the Ingress Queue Group Template Policy Select button in the Forwarding Plane Redirect panel to choose a policy. The Select Forwarding Plane Queue Group Instance form opens.

13 Choose a policy from the list and click on the OK button. The Select Forwarding Plane Queue Group Instance form closes. The L2 Access Interface (Create) form refreshes with the Ingress Queue Group Template Policy information displayed.

14 Configure the Instance ID parameter.



Note — The Instance ID parameter cannot be configured for Ipipe on Ethernet ports.

15 Configure the Egress Mark QinQ Top Bits Only parameter.

The Egress Mark QinQ Top Bits Only parameter is configurable only on Epipe L2 access interfaces.

16 Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - L2 Access Interface form opens.

17 Choose an egress QoS policy and click on the OK button. The Select Egress Policy - L2 Access Interface form closes and the L2 Access Interface (Create) form refreshes with the egress QoS policy information displayed.



Note — For Epipe and Ipipe VLL L2 access interfaces, if you select an access egress policy which has a forwarding class mapped to an egress queue group, you must ensure that the port you are configuring for the Epipe or Ipipe L2 egress interface has the access egress queue group with the same name created on it.

See Procedure 16-1 in chapter 16 for more information about how to configure Ethernet ports. See chapter 42 for more information about queue group template policies.

18 Click on the Select button in the Port Redirect panel to choose an Egress Queue Group Template Policy, if required. The Select Egress Queue Group Template Policy form opens.



Note — Selecting an Egress Queue Group Template Policy here permits the redirection of Ethernet traffic packets to a queue ID specified in the SAP's egress port queue group. The following properties and restrictions apply:

- If an Egress Queue Group Template Policy is specified here, the policy must have port redirection enabled.
- You cannot use policy-based redirection with the queue group when the SAP has SAP-based redirection enabled.
- Port access egress redirection is only supported on Ethernet/LAG ports. It is not supported on SAPs bound on non-Ethernet, Eth-tunnel, or CCAG ports.
- Supported ports include access, hybrid, and HSMDA.
- Queue groups can be applied to SAPs that incorporate LAGs. The LAGs can include port members from just a single card or from multiple cards.
- If you edit a LAG incorporated by the SAP, you cannot remove the last LAG member if a queue group reference exists to the containing SAP.
- You cannot add a secondary LAG member that has a queue group mismatch with primary LAG member.

19 Choose an Egress Queue Group Template Policy and click on the OK button. The Select Egress Queue Group Template Policy form closes, and the L2 Access Interface (Create) form refreshes with the Egress Queue Group Template Policy information displayed.

20 If you are configuring an L2 access interface for a 7710 SR or 7705 SAR, or if the port you selected in step 14 of Procedure 67-27 is not an HSMDA port, then go to step 28.

21 Configure the Packet Byte Offset (bytes) parameter, if required. You must enable the associated Override check box if you need to configure this parameter.

22 Click on the Select button in the Egress HSMDA Override panel to choose a WRR policy. The Select WRR Policy form opens.

23 Choose a WRR policy and click on the OK button. The Select WRR Policy form closes and the L2 Access Interface (Create) form reappears with the WRR policy information displayed.

24 Click on the Select button in the Egress HSMDA Override panel to choose an HSMDA egress secondary shaper policy. The Select Secondary Shaper form opens.

25 Choose a secondary shaper and click on the OK button. The Select Secondary Shaper form closes and the L2 Access Interface (Create) form reappears with the secondary shaper information displayed.

26 Configure the Use Shared Queue parameter. Go to step 28.

27 To configure a 7210 SAS NE perform the following steps.



Note — You can only assign policies and configure parameters for 7210 SAS NEs when the system resource profile is appropriately configured for the device. See "System resource profile" in chapter 8.

i Click on the Select button in the 7210 Specific panel to choose a SAS ingress policy. The Select SAS Ingress Policy - L2 Access Interface form opens.

ii Choose a SAS ingress policy and click on the OK button. The Select SAS Ingress Policy - L2 Access Interface form closes and the information is displayed.



Note — To support H-metering, you must choose a SAS ingress policy with all meter rate modes set to trtcm2.

iii Configure the following parameters in the Aggregate Rate Limit panel:

- Ingress Meter
- Ingress Meter Rate (kbps)
- Ingress Meter Burst
- Aggregate Shaper CIR Rate (kbps)
- Aggregate Shaper PIR Rate (kbps)



Note 1 — You can configure the Ingress Meter parameter only during SAP creation on the 7210 SAS-M, 7210 SAS-T, or 7210 SAS-X. The parameter must be set to true to support H-metering.

Note 2 — You can configure the Ingress Meter Rate (kbps) and Ingress Meter Burst parameters only after SAP creation on the 7210 SAS-M, 7210 SAS-T, or 7210 SAS-X.

28 Click on the OK button. The VLL L2 Access Interface (Edit) form closes and a dialog box appears.

29 Click on the Yes button. The *VLL_type* Service (Edit) form reappears.

30 Close the *VLL_type* Service (Edit) form.

31 Close the Manage Services form.

Procedure 67-29 To configure scheduling on a VLL L2 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VLL and click on the Properties button. The *VLL_type* Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface and choose Properties. The VLL L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Schedulers tab.



Note 1 — The Schedulers tab is configurable only if a port is assigned to the interface.

Note 2 — For the 7210 SAS-X, the port is enabled only when you select the SAP based type in the Egress Scheduler Mode.

8 To configure scheduling on a 7705 SAR site, perform the following steps. Otherwise, go to step 9.



Note 1 — For the 7705 SAR, scheduler behavior is determined by the scheduler mode, which is 4-Priority by default. You can only configure the Egress and Ingress Aggregate Rate Limit parameters when the Scheduler Mode parameter is set to 16-Priority. You can set the Scheduler Mode to 16-Priority only when the port is on an MDA that supports 16-Priority. See the 7705 SAR documentation for more information.

Note 2 — If you change the Scheduler Mode parameter from 16-Priority to 4-Priority, the 5620 SAM automatically restores the default settings for the Egress Aggregate Rate Limit and Ingress Aggregate Rate Limit panels when you click on the Apply or OK button.

i In the Egress Scheduler panel, configure the Scheduler Mode parameter.

ii In the Ingress Scheduler panel, configure the Scheduler Mode parameter.

iii If you set the Scheduler Mode parameter to 16-Priority in the Egress Scheduler panel or Ingress Scheduler panel, configure the parameters in the Egress Aggregate Rate Limit panel and Ingress Aggregate Rate Limit panel, as required. Otherwise, go to step 11.

- Assign Aggregate Rate Limit
- Aggregate Rate Limit (kbps)
- Assign Aggregate CIR
- Aggregate CIR (kbps)

iv Go to step 11.

9 Specify that an aggregation scheduler policy is not applied to the interface. To specify that an aggregation schedule is applied to the interface, go to step 10.

i Set the Aggregation parameter to off.



Note — The Aggregation parameter is not configurable if the port you selected in step 14 of Procedure 67-27 is an HSMDA port.

ii Configure the parameters:

- Aggregate Rate Limit (kbps)
- Frame-Based Accounting



Note 1 — The Aggregate Rate Limit (kbps) and Frame-Based Accounting parameters are configurable only when there is no scheduler specified in the Egress Scheduler panel.

Note 2 — The Frame-Based Accounting parameter is not configurable if the port you selected in step 14 of Procedure 67-27 is an HSMDA port.

Note 3 — You cannot specify an egress scheduler when the Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

iii Click on the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - L2 Access Interface form opens.

iv Choose an ingress scheduler and click on the OK button. The Select Ingress Scheduler - L2 Access Interface form closes, and the L2 Access Interface (Create) form refreshes with the ingress scheduler information displayed.

v If you are configuring this interface for an Ipipe service then go to step viii.

vi Click on the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Policer Control Policy form opens.

vii Choose a policer control policy and click on the OK button. The Select Policer Control Policy form closes and the VPLS L2 Access Interface (Create) form reappears with the ingress policer control policy information displayed.

viii If the port you selected in step 14 of Procedure 67-27 is an HSMDA port, go to step 11.

ix Click on the Select button in the Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - L2 Access Interface form opens.

x Choose an egress scheduler and click on the OK button. The Select Egress Scheduler - L2 Access Interface form closes, and the L2 Access Interface (Create) form refreshes with the egress scheduler information displayed.

xi If you are configuring this interface for an Ipipe service then go to step 11.

xii Click on the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Policer Control Policy form opens.

xiii Choose a policer control policy and click on the OK button. The Select Policer Control Policy form closes and the VPLS L2 Access Interface (Create) form reappears with the egress policer control policy information displayed.

xiv Go to step 11.

10 Specify that an aggregation scheduler policy is applied to the interface.

i Set the Aggregation parameter to On.



Note — You cannot specify an access scheduler policy if the port you selected in step 14 of Procedure 67-27 is an HSMDA port. Go to step 11.

ii Click on the Select button in the Aggregation Scheduler panel to choose an aggregation scheduler. The Select Aggregation Scheduler - L2 Access Interface form opens.

iii Choose an aggregation scheduler and click on the OK button. The Select Aggregation Scheduler - L2 Access Interface form closes, and the L2 Access Interface (Create) form refreshes with the aggregation scheduler information displayed.

11 Click on the OK button. The VLL L2 Access Interface (Edit) form closes and a dialog box appears.

12 Click on the Yes button. The *VLL_type* Service (Edit) form reappears.

13 Close the *VLL_type* Service (Edit) form.

14 Close the Manage Services form.

Procedure 67-30 To assign ingress and egress ACL filters to the VLL L2 access interface



Note 1 — IPv6 ACL filters are not supported on the 7705 SAR.

Note 2 — ACL filters are not supported for CPipe L2 access interfaces.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VLL and click on the Properties button. The *VLL_type* Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface and choose Properties. The VLL L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the ACL tab.

8 Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - L2 Access Interface form opens.

9 Choose an ingress ACL filter and click on the OK button. The Select Ingress Filter - L2 Access Interface form closes and the L2 Access Interface (Create) form reappears with the ingress ACL filter information displayed.

10 Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - L2 Access Interface form opens.

11 Choose an egress ACL filter and click on the OK button. The Select Egress Filter - L2 Access Interface form closes and the L2 Access Interface (Create) form reappears with the egress ACL filter information displayed.

12 Click on the Select button in the IPv6 Ingress Filter panel to choose an IPv6 ingress ACL filter. The Select IPv6 Ingress Filter - L2 Access Interface form opens.



Note — When you configure IPv6 ingress ACL filters on a 7210 SAS-E Release 5.0 R3 or later, you must configure the system resource profile appropriately on the device. See "System resource profile" in section 8.5 and Procedure 13-20 for more information.

13 Choose an IPv6 ingress ACL filter and click on the OK button. The Select IPv6 Ingress Filter - L2 Access Interface form closes and the L2 Access Interface (Create) form reappears with the IPv6 ingress ACL filter information displayed.

14 Click on the Select button in the IPv6 Egress Filter panel to choose an IPv6 egress ACL filter. The Select IPv6 Egress Filter - L2 Access Interface form opens.

15 Choose an IPv6 egress ACL filter and click on the OK button. The Select IPv6 Egress Filter - L2 Access Interface form closes and the L2 Access Interface (Create) form reappears with the IPv6 egress ACL filter information displayed.

16 Click on the OK button. The VLL L2 Access Interface (Edit) form closes and a dialog box appears.

17 Click on the Yes button. The *VLL_type* Service (Edit) form reappears.

18 Close the *VLL_type* Service (Edit) form.

19 Close the Manage Services form.

Procedure 67-31 To assign an accounting policy to a VLL L2 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VLL and click on the Properties button. The *VLL_type* Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface and choose Properties. The VLL L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Accounting tab.

8 Click on the Select button to choose an accounting policy. The Select Accounting Policy - L2 Access Interface form opens.

9 Choose an accounting policy and click on the OK button. The Select Accounting Policy - L2 Access Interface form closes, and the L2 Access Interface (Create) form refreshes with the accounting policy name.

10 Configure the Collect Accounting Statistics parameter.

11 If you are configuring statistics collection for a 7210 SAS, configure the following parameters. Otherwise, go to step 13.

- Enable Egress Packets Forwarding
- Ingress Counter Mode
- Ingress Counter Type

12 If you are configuring statistics collection for a 7210 SAS-D 6F 4T ETR, configure the following parameters. Otherwise, go to step 13.

- Enable Egress Forwarding
- Enable Ingress Forwarding

13 Click on the OK button. The VLL L2 Access Interface (Edit) form closes and a dialog box appears.

14 Click on the Yes button. The *VLL_type* Service (Edit) form reappears.

15 Close the *VLL_type* Service (Edit) form.

16 Close the Manage Services form.

Procedure 67-32 To assign a time of day suite to the VLL L2 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VLL and click on the Properties button. The *VLL_type* Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface and choose Properties. The VLL L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the TOD Suite tab.

8 Click on the Select button in the Time Of Day Suite panel. The Select Time Of Day Suite - L2 Access Interface list form opens.

9 Choose a time of day suite and click on the OK button. The Select Time Of Day Suite - L2 Access Interface list form closes, and the L2 Access Interface (Create) form reappears with the time of day suite name.



Note 1 — You cannot assign a ToD suite to a L2 access interface if accounting statistics collection is enabled on the L2 access interface. You must disable the Collect Accounting Statistics parameter in step 10 in Procedure 67-31.

Note 2 — SapEgrQosPlcyStats and SapIngQosPlcyStats statistics are only collected if a Time Of Day Suite is applied on the SAP.

10 Click on the OK button. The VLL L2 Access Interface (Edit) form closes and a dialog box appears.

11 Click on the Yes button. The *VLL_type* Service (Edit) form reappears.

12 Close the *VLL_type* Service (Edit) form.

13 Close the Manage Services form.

Procedure 67-33 To assign a DoS protection policy or DDoS protection policy to an Epipe or Ipipe L2 access interface



Note — A default DoS protection policy is automatically assigned to the interface.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VLL and click on the Properties button. The *VLL_type* Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface and choose Properties. The VLL L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Security tab.

8 Click on the Select button in the NE DoS Protection panel and select a DoS protection policy from the Select NE DoS Protection - L2 Access Interface form.

9 Click on the Select button next to the NE DDoS Protection Policy panel and select a DDoS protection policy from the Select NE DDoS Protection Policy - L2 Access Interface form.

10 Configure the MAC Monitoring parameter.

11 Click on the OK button. The VLL L2 Access Interface (Edit) form closes and a dialog box appears.

12 Click on the Yes button. The *VLL_type* Service (Edit) form reappears.

13 Close the *VLL_type* Service (Edit) form.

14 Close the Manage Services form.

Procedure 67-34 To associate a MEP with an Epipe or Apipe L2 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VLL and click on the Properties button. The *VLL_type* Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface and choose Properties. The VLL L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the ETH-CFM tab.

8 Click on the Create button in the MIP Configurations panel. The MIP Configurations (Create) form opens.

9 Configure the parameters in the MIP panel:

- Primary VLAN Enable
- VLAN ID
- MAC Address



Note — The Primary VLAN Enable, VLAN ID, and MAC Address parameters are configurable only when a port is assigned to the interface.

10 Click the OK button. The MIP Configurations (Create) form closes and a dialog box is displayed.

11 Click the OK button. The new MIP Configuration is displayed in the list.

12 As required, configure the Test Generation Options parameters:

- Role
- Use as Test Source
- Use as Test Target



Note — You can propagate test generation role settings to all MEPs on a SAP or service site using the Propagate to MEPs button.

13 Configure the Hold MEPs Up When SAP is Down parameter in the Hold MEP Up on SAP Failure panel, if required.



Note 1 — The Hold MEPs Up when SAP is Down parameter is configurable for L2 access interfaces on the 7705 SAR Release 6.0 R1 or later.

Note 2 — You can configure the Hold MEPs Up When SAP is Down parameter on only one SAP per node.

14 Click on the Create button in the MEPs panel. The MEP (Create) form opens with the General tab displayed.

15 Click on the Select button in the MEP panel to choose a MEG. The Select Maintenance Entity Group form opens.

16 Click the Search button and choose an entry, then click on the OK button. The Select Maintenance Entity Group form closes and information related to your selection is displayed on the form.

17 Configure the parameters in the MEP panel:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- Description
- MAC Address
- Primary VLAN Enable
- Type
- Interface Type



Note — The Type and Interface Type parameters are automatically populated based on whether the MEP is created on a SAP, SDP binding, or Ethernet Tunnel Path Endpoint.

18 Configure the parameters in the CCM panel:

- CCM Enabled
- Priority Level for CCM
- Fault Propagation
- CCM Padding Packet Size (Bytes)
- Low-priority Defect



Note — The CCM Padding Packet Size (Bytes) parameter cannot be configured when the CCM interval parameter is set to 10 ms or 100 ms.

19 Click on the Select button in the MEG Sub-Grouping panel to choose a MEG Sub-Group, if required. The Select MEG Sub-Group form opens.

20 Click the Search button and choose an entry, then click on the OK button. The Select MEG Sub-Group form closes, and your selection is displayed on the form.

21 As required, configure the Test Generation Options parameters:

- Role
- Use as Test Source
- Use as Test Target



Note 1 — The Test Generation Options parameters are only displayed when you set the Direction parameter to Up.

Note 2 — You can only configure Test Generation Options parameters for Epipe access interfaces.

22 If the MD for the MEP has a Maintenance Domain Name Type of none and the associated MEG has a Maintenance Entity group Name Type of icc-based, then the Y.1731 Tests and AIS tabs are configurable. Click on the Y.1731 Tests tab. Otherwise, go to step 26.

23 Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

24 Click on the AIS tab.

25 Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

26 Click on the OK button. A dialog box appears.

27 Click on the OK button. The MEP (Create) form closes.

28 Click on the OK button. The VLL L2 Access Interface (Edit) form closes and a dialog box appears.

29 Click on the Yes button. The *VLL_type* Service (Edit) form reappears.

30 Close the *VLL_type* Service (Edit) form.

31 Close the Manage Services form.

Procedure 67-35 To configure microwave compression on an MW link SAP associated with a 7705 SAR on the VLL L2 access interface



Note 1 — You can configure microwave compression only on an MW link SAP associated with a 7705 SAR-8 or 7705 SAR-18, Release 6.0 R1 or later.

Note 2 — Microwave compression cannot be configured on an MW link SAP when the Outer Encapsulation Value parameter of the port in step 15 of Procedure 67-27 is set to 0 or 1.

Note 3 — See Procedures 15-11 and 15-12 for more information about configuring a 7705 SAR MW link and MW link member.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VLL and click on the Properties button. The *VLL_type* Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface and choose Properties. The VLL L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Microwave tab.

8 Enable the Compression parameter.

9 Configure the parameters:

- Destination MAC
- Source MAC
- RTP

10 Click on the Apply button. A dialog box appears.

11 Click on the Yes button.

12 Click on the OK button. The VLL L2 Access Interface (Edit) form closes and a dialog box appears.

13 Click on the Yes button. The *VLL_type* Service (Edit) form reappears.

14 Close the *VLL_type* Service (Edit) form.

15 Close the Manage Services form.

Procedure 67-36 To configure an Ethernet tunnel on a VLL L2 access interface



Note — You can only configure an Ethernet tunnel if you are creating a same-fate SAP or a control/data SAP.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VLL and click on the Properties button. The *VLL_type* Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface and choose Properties. The VLL L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Ethernet Tunnel tab.

8 If you are configuring a fate-sharing Ethernet Tunnel Endpoint SAP (also referred to as same-fate SAP) then go to step 9. Otherwise, go to step 11.

9 Click on the Create button. The Ethernet Tunnel (Create) form opens.

10 Configure the parameters:

- Path ID
- Tag (Outer Encapsulation Value)
- Tag (Inner Encapsulation Value)

11 Click on the OK button. A dialog box appears.

12 Click on the OK button. The L2 Access Interface (Create) form refreshes with the Ethernet Tunnel entry.

13 Click on the OK button. The VLL L2 Access Interface (Edit) form closes and a dialog box appears.

14 Click on the Yes button. The *VLL_type* Service (Edit) form reappears.

15 Close the *VLL_type* Service (Edit) form.

16 Close the Manage Services form.

Procedure 67-37 To assign an ANCP policy to a VLL L2 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VLL and click on the Properties button. The *VLL_type* Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface and choose Properties. The VLL L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the ANCP Static Map tab. The ANCP Static Map (Create) form opens.

8 Configure the ANCP String parameter.

9 Click on the Select button to choose an ANCP Policy. The Select ANCP Policy - ANCP Static Map form opens.

10 Choose an ANCP policy and click on the OK button. The Select ANCP Policy - ANCP Static Map form closes and the ANCP Static Map form reappears with the ANCP policy information displayed.

11 Click on the OK button. The ANCP Static Map form closes.

12 Click on the OK button. The VLL L2 Access Interface (Edit) form closes and a dialog box appears.

13 Click on the Yes button. The *VLL_type* Service (Edit) form reappears.

14 Close the *VLL_type* Service (Edit) form.

15 Close the Manage Services form.

Procedure 67-38 To specify OAM functionality and assign ingress and egress ATM policies an Epipe, Apipe, or Ipipe L2 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VLL and click on the Properties button. The *VLL_type* Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface and choose Properties. The VLL L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the ATM tab.

8 Configure the parameters:

- AAL5 Encapsulation
- ATM OAM Alarm Cell Handling
- ATM OAM Terminate

The ATM OAM Terminate parameter is configurable only on Apipe L2 access interfaces. When the VLL access interface port belongs to a MC-APS channel and the VC Type parameter is set to ATM-SDU, set the ATM OAM Terminate parameter to Up.

The AAL5 Encapsulation parameter is configurable only on Epipe and Ipipe L2 access interfaces.

The ATM OAM Alarm Cell Handling parameter is configurable on Apipe L2 access interfaces only when the VC Type parameter is set to ATM-VCC or ATM-VPC, or when the VC Type parameter is set to ATM-cell and the ATM Connection Type parameter is set to PVC. The parameter is configurable on Epipe and Ipipe L2 access interfaces.

The ATM OAM Terminate is configurable on Apipe L2 access interfaces only when the VC Type parameter is set to ATM-SDU or ATM-VCC in step 4 of Procedure 67-8.

9 Click on the Select button in the Ingress ATM Policy panel to choose an ingress ATM policy. The Select Ingress ATM Policy - ATM Configuration form opens.

10 Choose an ingress ATM policy and click on the OK button. The Select Ingress ATM Policy - ATM Configuration form closes and the L2 Access Interface (Create) form reappears with the ingress ATM policy information displayed.

11 Click on the Select button in the Egress ATM Policy panel to choose an egress ATM policy. The Select Egress ATM Policy - ATM Configuration form opens.

12 Choose an egress ATM policy and click on the OK button. The Select Egress ATM Policy - ATM Configuration form closes and the L2 Access Interface (Create) form reappears with the egress ATM policy information displayed.

13 Click on the OK button. The VLL L2 Access Interface (Edit) form closes and a dialog box appears.

14 Click on the Yes button. The *VLL_type* Service (Edit) form reappears.

15 Close the *VLL_type* Service (Edit) form.

16 Close the Manage Services form.

Procedure 67-39 To specify the CEM functionality for an Epipe L2 access interface with CEM encapsulation



Note — Consider the following when creating a VLL Epipe L2 access interface with CEM encapsulation:

- The Time Slots parameter of the DS0 channel must be configured with at least one time slot.
- Time slots are automatically configured for unstructured E1 and T1 endpoints
- The Clock Source parameter of the DS1 channel must be set to Node-Timed.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VLL Epipe and click on the Properties button. The Epipe Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface and choose Properties. The VLL L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the CEM EPipe tab.

8 Configure the parameters:

- Jitter Buffer (ms)
- Payload Size (octets)
- RTP Header
- Report Alarm
- Local ECID
- Remote ECID
- Remote MAC Address

9 Click on the OK button. The VLL L2 Access Interface (Edit) form closes and a dialog box appears.

10 Click on the Yes button. The *VLL_type* Service (Edit) form reappears.

11 Close the *VLL_type* Service (Edit) form.

12 Close the Manage Services form.

Procedure 67-40 To specify the CEM functionality for the Cpipe L2 access interface



Note — Consider the following when creating a VLL Cpipe L2 access interface:

- The Time Slots parameter of the DS0 channel must be configured with at least one time slot.
- Time slots are automatically configured for unstructured E1 and T1 endpoints
- The Clock Source parameter of the DS1 channel must be set to Node-Timed.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VLL Cpipe and click on the Properties button. The Cpipe Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface and choose Properties. The VLL L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the CEM CPipe tab.

8 Configure the parameters:

- Jitter Buffer (ms)
- Payload Size (octets)
- Packetization Buffer (ms)
- RTP Header
- Report Alarm

9 Click on the OK button. The VLL L2 Access Interface (Edit) form closes and a dialog box appears.

10 Click on the Yes button. The *VLL_type* Service (Edit) form reappears.

11 Close the *VLL_type* Service (Edit) form.

12 Close the Manage Services form.

Procedure 67-41 To switch to the redundant port for a VLL SAP from an L2 access interface properties form

Perform this procedure from a port properties form when port redundancy is configured on one or more a Cpipe or Epipe SAPs to:

- switch to the backup port or channel assigned to the SAP, for example, in the event of a fault on the primary port or channel
- switch back to the primary port or channel assigned to the SAP, for example, after a fault condition on the primary is cleared



Caution — Alcatel-Lucent recommends that you set the OLC state of a service to Maintenance before you switch to a redundant port or channel, and reset the port to the previous state after the switch is complete.



Note 1 — When multiple SAPs are selected, switching is attempted only for the SAPs that support port redundancy and on which port redundancy is properly configured.

Note 2 — Port redundancy switching fails if the SAP or port is included in one of the following redundancy objects:

- BGP-MH
- MC-APS
- MC-LAG
- MC-ring

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VLL Cpipe or Epipe service and click on the Properties button. The *VLL_type* Service (Edit) form opens with the General tab displayed.

4 Expand the Site object in the service navigation tree.

5 Expand the L2 Access Interfaces object in the service navigation tree.

6 Click on the SAP object in the service navigation tree. The Port (Edit) form appears with the General tab displayed.

7 Click on the Port tab.

8 Click on the Switch to Redundant SAP button. A dialog box appears.

9 Click on the OK button. The Port (Edit) form closes and a dialog box appears indicating that the SAP object on the current site is removed.

10 Click on the OK button.

11 Verify the following:

- For on-node switching, the SAP is deleted from the primary port, and a new SAP is created on the site.
- For off-node switching, the SAP and the parent site are deleted, and a new site, SAP, and spoke SDP bindings are created for the service.

12 Choose the SAP in the navigation tree. The Port (Edit) form opens with the General tab displayed.

13 Click on the Port tab. The Manual Switch Backup State indicator displays one of the following:

- Backup SAP in Use, if you switch from primary to backup
- Backup Port Specified, if you switch from backup to primary



Note — When the Manual Switch Backup State indicator reads Backup SAP in Use, the displayed port redundancy information is for the primary port of the SAP, and is read-only.

14 Close the Port (Edit) form.

15 Close the *VLL_type* Service (Edit) form.

16 Close the Manage Services form.

Procedure 67-42 To switch to the redundant port for one or more VLL SAPs from a service, site, or port properties form

Perform this procedure from a service or site properties form when port redundancy is configured on one or more a Cpipe or Epipe SAPs to:

- switch to the backup port or channel assigned to the SAP, for example, in the event of a fault on the primary port or channel
- switch back to the primary port or channel assigned to the SAP, for example, after a fault condition on the primary port or channel is cleared



Caution — Alcatel-Lucent recommends that you set the OLC state of a service to Maintenance before you switch to a redundant port or channel, and reset it to the previous state after the switch is complete.



Note 1 — When multiple SAPs are selected, switching is attempted only for the SAPs that support port redundancy and on which port redundancy is properly configured.

Note 2 — Port redundancy switching fails if the SAP or port is included in one of the following redundancy objects:

- BGP-MH
- MC-APS
- MC-LAG
- MC-ring

1 Perform one of the following.

a Choose the SAPs from a port properties form:

i Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

ii Choose Port from the Select Object Type drop-down menu.

iii Configure the search criteria, as required, and click on the Search button. A list of ports appears.

iv Choose the required port from the list and click on the Properties button. The Physical Port (Edit) form opens with the General tab displayed.

v Click on the L2 Access Interfaces tab.

vi Click on the Search button. A list of all of the SAPs that are configured on the port is displayed.

vii Choose the required SAPs and click on the Properties button. The L2 Access Interface (Edit) form opens with the General tab displayed.

viii Click on the Port tab.

ix Go to step 6.

b Go to step 2 to choose the SAPs from a service or site properties form.

2 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

3 Configure the filter criteria. A list of services appears.

4 Choose the required VLL Cpipe or Epipe service and click on the Properties button. The *VLL_type* Service (Edit) form opens with the General tab displayed.

5 Perform one of the following.

a Choose the SAPs from a list of all SAPs in the service.

i Click on the L2 Access Interfaces tab. A list of SAPs that are configured on the service is displayed.

ii Choose the required SAPs.

b Choose the SAPs from a list of all of the SAPs on a site.

i Expand the Sites object in the service navigation tree.

ii Click on the site object. The Site (Edit) form opens with the General tab displayed.

iii Click on the Interfaces tab.

iv Click on the L2 Access Interfaces tab. A list of all SAPs on the site is displayed.

v Choose the required SAPs.

6 Click on the Switch to Redundant SAP button. A dialog box appears.

7 Click on the OK button. The selected SAPs in the list are deleted, and new SAPs are created on the redundant port.

8 To confirm the redundancy status of a SAP, perform the following steps.

i Choose the SAP in the list and click on the Properties button. The Port (Edit) form opens with the General tab displayed.

ii Click on the Port tab. The Manual Switch Backup State indicator displays one of the following:

- Backup SAP in Use, if you switch from primary to backup
- Backup Port Specified, if you switch from backup to primary



Note — When the Manual Switch Backup State indicator reads Backup SAP in Use, the displayed port redundancy information is for the primary port of the SAP, and is read-only.

9 Close the Port (Edit) form.

10 Close the *VLL_type* Service (Edit) form.

11 Close the Manage Services form.

Procedure 67-43 To create a SAP aggregation group

Perform this procedure to create a SAP aggregation group on a 7705 SAR Apipe service.



Note — SAP aggregation groups can be created only on Apipe services that are configured with the ATM VCC or ATM N:1-N>1 VC Type option. See Procedure 67-8 for more information about configuring the VC type.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria, if required, and click on the Search button.

3 From the list, choose an Apipe service with at least one 7705 SAR site and click on the Properties button. The Apipe Service (Edit) form opens with the General tab displayed.

4 From the service navigation tree, expand to the site level and click on a 7705 SAR site. The Apipe Site (Edit) form opens with the General tab displayed.

5 Click on the Aggregation Group tab.

6 Click on the Create button. The SAP Aggregation Group (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Description
- Aggregation Group

8 Click on the QoS tab.

9 Specify an ingress policy for the SAP aggregation group:

i Click on the Select button in the Ingress Policy panel. The Select Ingress Policy - SAP Aggregation Group form opens.

ii Configure the filter criteria, if required, and click on the Search button.

iii Choose an ingress policy and click on the OK button. The Select Ingress Policy - SAP Aggregation Group form closes.

10 Specify an egress policy for the SAP aggregation group:

i Click on the Select button in the Egress Policy panel. The Select Egress Policy - SAP Aggregation Group form opens.

ii Configure the filter criteria, if required, and click on the Search button.

iii Choose an egress policy and click on the OK button. The Select Egress Policy - SAP Aggregation Group form closes.

11 Click on the Accounting tab.

12 Specify an accounting policy for the SAP aggregation group:

i Click on the Select button in the Accounting Policy panel. The Select Accounting Policy - SAP Aggregation Group form opens.

ii Configure the filter criteria, if required, and click on the Search button.

iii Choose an accounting policy and click on the OK button. The Select Accounting Policy - SAP Aggregation Group form closes.

13 Click on the OK button. The SAP Aggregation Group (Create) form closes.

14 From the service navigation tree, expand the entries of the 7705 SAR site.

15 Right-click on the newly created SAP Aggregation Group entry and choose Create L2 Access Interface from the contextual menu. The L2 Access Interface (Create) form opens with the General tab displayed.

16 Configure the parameters:

- Description
- Administrative State

17 Click on the Port tab.

18 Specify a terminating port for the L2 access interface:

i Click on the Select button in the Termination Port panel. The Select Terminating Port - L2 Access Interface form opens.

ii Configure the filter criteria, if required, and click on the Search button.

iii Choose a port from the list and click on the OK button. The Select Terminating Port - L2 Access Interface form closes.

19 Configure the parameters:

- Outer Encapsulation Value (VPI)
- Inner Encapsulation Value (VCI)

20 Click on the ATM tab.

21 Configure the parameters:

- ATM OAM Alarm Cell Handling
- Subscriber Vlan
- Translated VPI
- Translated VCI

22 Assign an Ingress ATM Policy to the L2 access interface:

i Click on the Select button in the Ingress ATM Policy panel. The Select Ingress ATM Policy - ATM Configuration form opens.

ii Configure the filter criteria, if required, and click on the Search button.

iii Choose a policy from the list and click on the OK button. The Select Ingress ATM Policy - ATM Configuration form closes.

23 Assign an Egress ATM Policy to the L2 access interface:

i Click on the Select button in the Egress ATM Policy panel. The Select Egress ATM Policy - ATM Configuration form opens.

ii Configure the filter criteria, if required, and click on the Search button.

iii Choose a policy from the list and click on the OK button. The Select Egress ATM Policy - ATM Configuration form closes.



Note — The QoS and Accounting tabs are dimmed when an L2 access interface is assigned to a SAP aggregation group. The QoS and accounting policies that are assigned to the SAP aggregation group are automatically assigned to all of the SAPs in the group.

24 Click on the OK button. The L2 Access Interface (Create) form closes.

25 Repeat steps 15 to 24 to create more SAPs, as required.



Note 1 — A SAP aggregation group can contain up to 16 SAPs.

Note 2 — Alternatively, you can create SAPs for a SAP aggregation group by right-clicking on the L2 Access Interfaces entry and choosing the newly created SAP aggregation group.

26 Close all forms.

Procedure 67-44 To create an HSDPA resiliency configuration

See "HSDPA Offload Resiliency" in section 67.1 for information about HSDPA resiliency.

1 Choose Manage→Redundancy→HSDPA Resiliency from the 5620 SAM main menu. The HSDPA Resiliency Manager form opens.

2 Click on the Create button. The HSDPA Resiliency (Create) form opens.

3 Configure the parameters:

- Description
- Administrative State

4 Click the Select button beside the Name parameter in the Site panel. The Select Site - HSDPA Resiliency form opens. Only sites utilizing a 7705 SAR chassis are displayed.

5 Choose a site and click on the OK button. The Select Site - HSDPA Resiliency form closes and the HSDPA Resiliency (Create) form is displayed with your site choice shown in the Name parameter field.

6 Click the Select button beside the Name parameter in the Primary Service panel. The Select Primary Service - HSDPA Resiliency form opens with a list of services.



Note — The Select Primary Service - HSDPA Resiliency form does not give you the option to create the required Apipe service. See Procedure 67-8 to create the required service before configuring HSDPA Resiliency.

7 Choose a service and click on the OK button. The HSPDA Resiliency (Create) form refreshes with the primary service information.

8 Click the Select button beside the Name parameter in the Secondary Service panel. The Select Secondary Service - HSDPA Resiliency form opens with a list of services.



Note — The Select Secondary Service - HSDPA Resiliency form does not give you the option to create the required Apipe service. See Procedure 67-8 to create the required service before configuring HSDPA Resiliency.

9 Choose a service and click on the OK button. The HSPDA Resiliency (Create) form refreshes with the secondary service information.

10 Click on the OK button. The HSDPA Resiliency (Create) form closes.

11 Perform one of the following:

a Perform Procedure 67-45 to turn up or manually operate an HSDPA resiliency configuration.

b Close the HSDPA Resiliency Manager form.

Procedure 67-45 To activate and manually operate an HSDPA resiliency configuration

See section "HSDPA Offload Resiliency" for more information.

1 Choose Manage→Redundancy→HSDPA Resiliency from the 5620 SAM main menu. The HSDPA Resiliency Manager form opens.

2 Choose the required HSDPA resiliency configuration from the displayed list and click the Properties button. The HSDPA Resiliency (Edit) form opens with the properties of the configuration displayed on the General tab.

The Active Service field displays whether the Primary or Secondary Service is active. When you initially want to turn up a resiliency configuration, typically Primary is displayed.

3 Set the Administrative State parameter to Disabled. Activity for the resiliency configuration can only be manually switched from this form when this parameter is set to Disabled.

4 Perform one of the following:

a Set the Administrative State parameter to Enabled. Activity automatically switches between the primary and secondary services as required when this parameter is enabled.

b Click on the Turn Up button to manually activate the HSDPA resiliency configuration. Do this if the Administrative State parameter is not enabled.

c If the Primary Service is currently active, you can click on the Force Secondary Service Active button. This manually forces the configuration to the Secondary Service (if up), regardless of state of damping timer. The Active Service field displays Secondary if the switchover is successful.

d If the Secondary Service is currently active, you can click on the Force Primary Service Active button. This manually forces the configuration to the Primary Service (if up), regardless of state of damping timer. The Active Service field displays Primary if the switchover is successful.

e Click on the Shut Down button to de-activate the HSDPA resiliency configuration.

f Click on the Faults tab to view and address alarms related to the configuration.

5 Click on the OK button. The HSDPA Resiliency (Edit) form closes.

6 Close the HSDPA Resiliency Manager form.

Procedure 67-46 To run an OAM validation test for a VLL service

An OAM validator test suite must be created for the tested entity. See chapter 77 for more information about how to create a validator test suite.



Note — As an alternative, you can also run an OAM validation test on the service by performing a One Time Validation. This is a mostly automated procedure and is described in Procedure 77-9.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a service and click on the Properties button. The VLL *Type_of_VLL* (Edit) form opens with the General tab displayed.

4 Click on the Validate button. If the Validate button is not visible, click on the More Actions button and choose Validate. If an OAM validator test suite is not associated to the service, a dialog box appears. Perform the following steps:

   i Click on the OK button to associate the service with an existing OAM validator test suite. The Choose Validator Test Suite form appears.

   ii Configure the filter criteria. A list of OAM validator test suites appears.

   iii Choose an OAM validator test suite and click on the OK button. The Choose Validator Test Suite form closes.

5 View the State Cause indicators. When the validation test fails, a check mark appears beside the OAM Validation Failure indicator.

6 Click on the Tests tab. The Test Suite tab is displayed.

7 Click on the Tested Entity Result tab.

8 Choose an entry and click on the Properties button. The Tested Entity Result (Edit) form opens with the General tab displayed.

9 Click on the Results tab to display the validation test results.

10 If you need to compare two test results from the same type of test, choose the two test results and click on the Compare button; the Difference form opens. Otherwise, go to step 13.

11 Compare the test results.

12 Close the Difference form.

13 Close the Tested Entity Result form.

14 Close the VLL *Type_of_VLL* (Edit) form.

15 Close the Manage Services form.

Procedure 67-47 To view the service topology associated with a VLL service

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter parameters and click on the Search button. A list of services appears.

3 Choose a VLL service and click on the Topology View button. A Topology View dialog box appears.

4 Click on the Yes button to proceed. The Service Topology - *Service Name* map opens.

See chapter 6 for more information about service topology views.

Procedure 67-48 To view the VLL service operational status

The Operational State and State Cause indicators on the General tab of the service management form display information about service faults.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a service and click on the Properties button. The VLL *Type_of_VLL* (Edit) form opens.

4 View the Operational State and State Cause indicators. When the Operational State is Down, a check mark beside the appropriate State Cause indicator identifies the type of associated service fault.

5 Click on the appropriate tab to view or edit an object that is identified as faulty by a State Cause indicator.

6 Click on the Faults tab to view the alarms for the object. The Object Alarms tab is displayed.

7 Click on the Aggregated Alarms tab to view the aggregated alarms for the object. The Aggregated Alarms tab is displayed.

8 Close the VLL *Type_of_VLL* (Edit) form.

9 Click on the Close button to close the Manage Services form.

Procedure 67-49 To view the local PW status information for a VLL service

Perform this procedure to view the state cause information for the near end of a VLL spoke SDP binding.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose the service and click on the Properties button. The VLL *Type_of_VLL* (Edit) form opens.

4 Click on the Spoke SDP Bindings tab.

5 Select an entry and click on the Properties button. The Spoke SDP Binding (Edit) form opens.

6 Click on the States tab.

7 View the information in the Local State Cause panel. When there is a local fault, a check mark beside the appropriate indicator identifies the fault type.

8 Close the Spoke SDP Binding (Edit) form.

9 Close the VLL *Type_of_VLL* (Edit) form.

Procedure 67-50 To view the peer PW status information for a VLL service

Perform this procedure to view the state cause information for the far end of a VLL spoke SDP binding.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose the service and click on the Properties button. The VLL *Type_of_VLL* (Edit) form opens.

4 Click on the Spoke SDP Bindings tab.

5 Choose an entry and click on the Properties button. The Spoke SDP Binding (Edit) form opens.

6 Click on the States tab.

7 View the peer status information in the Peer State Cause panel. When the service tunnel or peer SAP is down or partially down, a check mark beside the appropriate indicator identifies the fault type.

8 Close the Spoke SDP Binding (Edit) form.

9 Close the VLL *Type_of_VLL* (Edit) form.

Procedure 67-51 To modify a VLL service



Caution — Modifying parameters can be service-affecting.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VLL service and click on the Properties button. The *VLL_type* Service (Edit) form opens with the general properties of the service displayed on the General tab.

The following tabs list the service elements that can be individually or collectively selected and configured:



Note 1 — Users with the administrator scope of command role can click on the Select button on the Template tab to associate a service template with the service object, if required.

Note 2 — Some service element do not apply to all VLL services.

- Bandwidth tab — displays service tunnel bandwidth booking information for the service.
- Sites tab — lists the sites that are included in the service
- Endpoints tab — lists the service endpoints
- Interface tab — lists the access interfaces that are included in the service
- Spoke SDP Bindings tab — displays the spoke SDP bindings that are associated with the service
- VLAN Path Instance - list VLAN path instances associated with a 9500 MPR service
- Template tab — displays the template used to create the service, if applicable.
- Tests tab
- Faults tab — displays the faults associated with the service



Note — Users with the administrator scope of command role can click on the Select button on the Template tab to associate a service template with the service object, if required.

4 Modify the parameters for the service as required.

To configure items on the tabs that contain lists of service elements, select the items and click on the Properties button.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button to confirm the action. The *VLL_type* Service (Edit) form closes and the Manage Services form reappears.

7 Click on the Close button to close the Manage Services form.

Procedure 67-52 To modify a VLL service using the topology view

The topology view for a service provides a graphical representation of the various components and their interconnections. You can also use this view to add, modify, or just navigate to service components. This provides an alternative approach to performing these functions from the navigation tree view.

Working from the topology view can expedite the creation of the components, since many of the fields you would ordinarily have to set in the configuration forms will be automatically populated using this approach. The configuration forms can also be accessed directly at any time from this view by right-clicking on a component. This allows quick access to conduct more detailed component configuration.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VLL and click on the Topology View button. The Service Topology map opens.

The remainder of this procedure contains a number of sub-procedures describing the various components that can be created and modified from the topology view. These include:

- Creating a new site. Go to step 4.
- Creating site components. Go to step 9.
- Creating spoke SDP bindings. Go to step 19.

Adding a new site

4 Right-click on any blank space in the service topology map. A contextual menu is displayed. Choose the option allowing you to create a new site. This may be an Epipe, Cpipe, Ipipe, Apipe, or Fpipe site, depending on what type of VLL service you are modifying.

The Select Network Elements form appears.

5 Choose one or more sites to add to the service and click on the OK button. The Site (Create) form for the new site is displayed. If you selected more than one site, the Site (Multiple Instances) (Create) form for the new sites is displayed.

6 Click on the OK button. The Site (Create) (or Site (Multiple Instances) (Create)) form closes and the new site (or sites) is displayed on the map.

7 If you want to perform detailed configuration of site properties for the new site, right-click on the site icon and select Properties from the contextual menu. The Site (Edit) form opens. Refer to Procedures 67-2 through 67-22 for detailed site configuration information for the various types of VLL services.

8 Return to step 3 for a list of other functions you can perform from the topology view or go to step 27 to finish.

Creating site components

9 Right-click on a site icon or a SAP aggregation group icon in the service topology map. A contextual menu is displayed. Depending on the service type and the icon you clicked on, you can choose to create one of the following:

- Endpoint. Go to step 10.
- L2 Access Interface. Go to step 13.
- SAP Aggregation Group. Go to step 16.

10 If you choose to create an Endpoint, the Endpoint (Create) form is displayed.

11 Configure the Name parameter for the endpoint.

Refer to Procedures 67-2 through 67-21 and 67-27 for detailed information about further configuring the endpoint, if required.

12 Click on the OK button. The Endpoint (Create) form closes and the new endpoint is displayed in the topology view.

13 If you choose to create an L2 Access Interface, then the L2 Access Interface (Create) form is displayed.

14 Click on the Port tab and assign a port to the interface.

Refer to Procedures 67-2 through 67-22 and 67-27 for detailed information about further configuring the interface, as required.

15 Click on the OK button. The L2 Access Interface (Create) form closes.

16 If you choose to create a SAP aggregation group, then the SAP Aggregation Group (Create) form is displayed.

17 Refer to Procedure 67-43 for detailed information about configuring the SAP aggregation group.

18 Return to step 3 for a list of other functions you can perform from the topology view or go to step 27 to finish.

Creating spoke SDP bindings

19 Choose the sites you want to connect in the service topology map and right-click on any one of them. A contextual menu is displayed.



Note — When you create a spoke binding between two sites, the order in which you select them is important. The first site you select will become the source site and the second site will become the destination site. Therefore, it is not recommended that you do a marquee-select in the topology view, since you will not be sure of this hierarchy. Instead, select the sites individually, and hold down the Shift or Ctrl key after your first selection.

20 Choose Connect from the contextual menu and choose the Create Spoke SDP Binding option.

The Spoke SDP Binding (Create) form is displayed.



Note 1 — For this function, it is assumed that you clicked on the source site first and then held down the Shift or Ctrl key while right-clicking on the destination site to display the contextual menu.

Note 2 — You can also create a spoke SDP binding between a site icon and an endpoint icon, or between two endpoint icons in the topology view. Appropriate endpoints must first exist or be created to enable this.

21 Enable the Auto-Select Transport Tunnel parameter.

22 You can manually configure other parameters here if required, or click on the OK button. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Spoke SDP Binding (Create) form closes and the new binding between the two sites is displayed in the topology view. Refer to Procedures 67-2 through 67-21 for more detailed information about creating and configuring spoke SDP bindings for the various types of VLL services, if required.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. Refer to Chapter 27 for information about how to create the required tunnel. When the tunnel is created, you can repeat this sub-procedure.

23 Assuming that the spoke SDP binding was successfully created in step 22, select the same two sites again in the topology view, although this time do so in the opposite order that you originally selected them. This will allow you to create a spoke binding for the return tunnel.

24 Right-click on the second site you selected and choose the Create Spoke SDP Binding... option from the contextual menu. The Spoke SDP Binding (Create) form is displayed.

25 You can manually configure other parameters here if required, or click on the OK button. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Spoke SDP Binding (Create) form closes and the new return binding between the two sites is displayed in the topology view.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. Refer to Chapter 27 for information about how to create the required tunnel. When the tunnel is created, you can repeat this sub-procedure.

26 Return to step 3 for a list of other functions you can perform from the topology view or go to step 27 to finish.

27 Close the Service Topology form.

28 Close the Manage Services form.

Procedure 67-53 To delete a VLL service



Warning — Deleting a service may result in a service disruption for customers. Consider the implication of deleting the service before proceeding.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 As required, configure the filter criteria to locate the service or range of services to be deleted. A list of services appears.

3 Choose a service or a range of services from the list.

4 Click on the Delete button. A warning form appears. This message is dynamic based on the priority of the service. Perform one of the following:

a For services with a low priority, go to Step 5.

b For services with a medium priority, configure the “Enter the highest priority of the service being deleted” text field by typing: Medium. Go to Step 5.

c For services with a high priority, configure the “Enter the highest priority of the service being deleted” text field by typing: High. Go to step 5.

5 For all services regardless of how their priority is configured, acknowledge the check box that prompts you confirm that you understand the implications of deleting the service.



Note — If you select multiple services with different priorities, you must enter the highest priority level of selected services before you can delete the services.

6 Click on the Yes button to confirm the action. The service is deleted and removed from the list.

7 Click on the Close button to close the Manage Services form.

Procedure 67-54 To create a BGP VPWS

1 Enable and configure BGP on the nodes involved in the BGP VPWS. See Section 23.16 for information about configuring BGP.

2 Create and distribute a Service PW template policy to the nodes involved in the VPWS. See Chapter 73 for information about using Service PW template policies.

3 Create an Epipe service. See Procedure 67-1 for information about creating an Epipe service.

4 Create the Epipe sites for the BGP VPWS. See Procedure 67-2 for information about creating an Epipe site.

5 Select one of the Epipe sites you created in step 4. The Site Epipe Service (Edit) form appears.

6 Click on the BGP tab.

7 Configure the parameters in the General tab:

- Enable BGP
- Route Distinguisher
- Import Route Target
- Export Route Target

8 Perform the following to create a PW Template Binding for the site.

i In the PW Template Binding panel, click on the Create button. The PW Template Binding form appears.

ii In the PW Template panel, click on the Select button and choose the Service PW Template policy you created in step 2.

iii Click on the PW Template Binding Route Target tab.

iv Click on the Create button to create a route target. The PW Template Route Target form appears.

v Configure the Import Route Target parameter, and click on the OK button. The new route target appears in the list.

vi Click on the OK button. The PW Template Binding form closes, and the new template binding appears in the list.

9 Configure the parameters in the VPWS tab:

- Enable BGP VPWS
- VE Name
- VE ID
- Administrative State

10 Perform the following to create a remote VE instance:

i In the Remote VE Instances panel, click on the Create button. The BGP VPWS Remote VE (New) form appears.

ii Configure the parameters:

- Remote VE Name
- Remote VE ID



Note — You can only create one remote VE instance for sites on 7450 ESS, 7710 SR, 7750 SR, or 7950 XRS nodes using Release 11.0 R1. Multiple remote VE instances can be created for sites on nodes with Release 11.0 R4 or later installed.

11 Click on the Apply button.

12 Repeat steps 5 to 11 for each site in the VPWS. When the sites have been configured, endpoints and associated spoke SDP bindings are automatically created by the nodes.



Note — Endpoints are not automatically created on 7450 ESS, 7710 SR, 7750 SR, or 7950 XRS nodes using Release 11.0 R1 to R3. Instead, only the spoke SDP bindings are created. See Procedure 67-26 for information about creating endpoints.

68 — VPLS management

68.1 VPLS management overview *68-2*

68.2 Sample VPLS configuration *68-30*

68.3 Workflow to create a VPLS *68-37*

68.4 VPLS management procedures *68-41*

68.1 VPLS management overview

VPLS is a class of virtual private network multipoint L2 service that allows multiple customer sites to be connected in a single bridged domain contained within the service provider-managed IP/MPLS network. Customer sites in the VPLS appear to be on the same LAN, even if the sites are geographically dispersed.

VPLS offers the following advantages:

- Ethernet interfaces on the host access side simplify provisioning.
- All routers in the VPLS are part of the same LAN, which simplifies IP addressing and allows customers to control and simplify their routing strategies.
- VPLS is protocol independent, which means there is no L2 protocol conversion between LAN and WAN technologies.

A VPLS can span a single site or multiple sites. A VPLS that spans a single site is called a local VPLS. In a local VPLS, customer data enters the service through multiple access interfaces on a single PE device. No circuit provisioning is required for the local VPLS.

A VPLS that spans multiple sites is called a distributed VPLS. In a distributed VPLS, customer data enters the service using two or more interfaces on different PE devices. The VPLS is transported by service circuits over an IP/MPLS provider core network carried by service tunnels. Service tunnels are created using GRE or MPLS LSPs.

You can use HVPLS to eliminate the need for a full mesh of virtual circuits between devices in the VPLS. See "HVPLS" in this section for more information.

The 5620 SAM supports end-to-end VPLS configuration using the following methods:

- Tabbed configuration forms with an embedded navigation tree. The navigation tree provides a logical view of the service and acts as a configuration interface.
- Pre-configured template. A user who is assigned the template management role can create a service template. See "Managing templates" in the *5620 SAM Scripts and Templates Developer Guide* for more information about the administrative tasks associated with service templates.

The General tab of the 5620 SAM service management form displays useful information about the operational state of the service and its sites through the Aggregated Operational State and State Cause indicators.

The Aggregated Operational State indicator has four possible values: Up, Down, Partially Down, and Unknown. The value is derived from the operational states of the sites that are part of the service, as follows:

- Up—all sites are operationally up
- Partially Down—at least one site is operationally down
- Down—all sites are operationally down
- Unknown—the service has no provisioned sites

When the Aggregated Service Site Operational State is Partially Down or Down, a check mark appears beside the appropriate State Cause indicator to identify the type of fault to the 5620 SAM operator. Alarms can be viewed on the Faults page.

When you use the 5620 SAM to create or discover a service, the 5620 SAM assigns a default tier value to the service. The Service Tier parameter value is relevant only in the context of composite service topology map views. See chapter 74 for more information about the hierarchical organization of composite services.

Common to all services, such as VPLS, are policies that are assigned to the service. Policies are defined at a global level and can then be applied to components of the service, such as interfaces and circuits, when the service is configured or modified. The following policies are common to all services:

- QoS policies to define ingress classification, policing, shaping, and marking on the ingress side of the interface. QoS policies are configured using the Access Ingress Policy Manager and the Access Egress Policy Manager.
- Policer control policies to control access ingress policers and access egress policers under a common hierarchy. Policer control policies are configured using the Policer Control Policy Manager.
- Scheduling policies to define hierarchical rate limiting and scheduling to govern the scheduling of queues. Scheduler policies are configured using the Scheduler Policy Manager.
- Port scheduler policies define hierarchical bandwidth allocation and scheduling at the egress port level. Port scheduler policies are configured using the Port Scheduler Policy and HSMDA Scheduler Policy forms.
- Filter policies to control network traffic into or out of an interface or circuit based on IP or MAC matching criteria. Filter policies are configured using the ACL IP Filter Manager and the ACL MAC Filter Manager.
- Accounting policies to count the traffic on a service to ensure proper billing and enforcement of SLAs. Accounting policies are configured using the Accounting Policy Manager.
- ANCP policies provide status and control information based on port-up and port-down messages and current line rate changes between the edge device and the access node. ANCP policies are configured using the Manage Subscriber Policies form.
- Time of day suites specify time and day restriction policies that are assigned to QoS policies and schedulers, ACL filters, and aggregation schedulers. Time of day suites and time range policies are configured using the Time of Day Suite form and Time Range form, respectively.

See chapter 42 for more information about policies.

Packets that arrive at an edge device are associated with a VPLS based on the access interface on which they arrive. An access interface is uniquely identified using the following parameters:

- physical Ethernet port or POS port and channel
- encapsulation type
- encapsulation identifier (if required)

If there are service issues, the service provider can use OAM tools to troubleshoot service and network transport issues, and ensure problems are handled properly through the physical and logical network. See chapter 32 for more information.

To provide a VPLS over an MPLS infrastructure, the device is configured to provide bridging and replication for each VPLS. The routers that are part of the VPLS are connected by MPLS LSPs. Multiple VPLS can use the same set of service tunnels. Multiple service tunnels can rely on multiple LSPs. The signaling is specified in sets of ingress and egress VC labels for each VPLS.

The following additional features are configured for the VPLS:

- MAC learning for the access ports and tunnels, including filtering based on MAC addresses on a per SAP basis
- MAC learning protection on SAPs to prevent DoS attacks from sourcing
- rate limiting of broadcast, destination unknown, and multicast traffic on a per access port basis
- FIB for each VPLS, including FIB size limits, static MAC addresses, alarms, and discarding unknown locations
- optional support for spanning tree for loop detection
- GSMP for each VPLS
- L2 management interfaces for each VPLS

You can run an OAM Validation test suite for the service by clicking on the Validate button. If the Validate button is not visible, click on More Actions and choose Validate. Alternatively, you can also perform a One Time Validation. If a check mark appears beside the OAM Validation Failed state cause indicator, the test has failed. In addition, the Tested Entity Result tab on the Tests tab displays detailed information about the OAM test result. OAM validation tests are not supported for HVPLS. See chapter 77 for more information about how to configure OAM validation test suites.

HVPLS

A hierarchical VPLS is created by enhancing the VPLS core mesh with a spoke SDP binding that is connected to another site in the same VPLS, a site in another VPLS, or a VLL site.

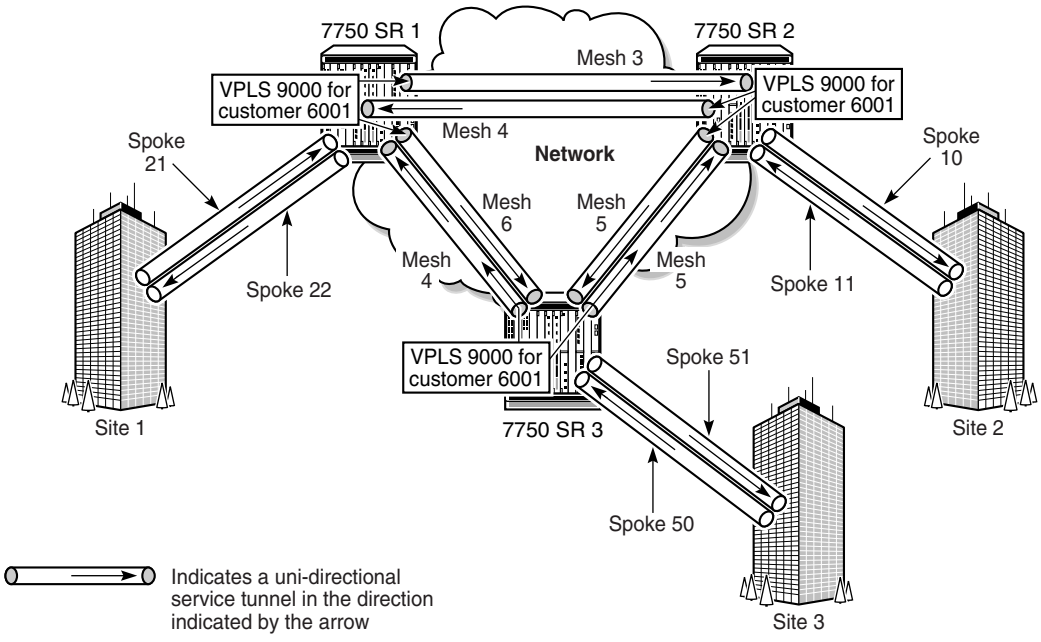
HVPLS offers the following advantages:

- reduces the complexity of mesh configuration
- decreases the amount of signaling of routes between devices

When traffic arrives at an access-spoke circuit, it acts like a bridge port where flooded traffic received on the access spoke is replicated to all other spokes, meshes, or SAPs but it is not transmitted on the port where it is received.

Figure 68-1 shows a sample HVPLS with a mesh and spoke configuration. Spokes 50 and 51 are unidirectional access-spoke circuits bound to service tunnels. The access-spoke circuits exist within the context of a VLL service or VPLS that is interconnected to the original, fully meshed VPLS. Alternatively, the access-spoke circuit can provide interconnectivity to a service site.

Figure 68-1 HVPLS configuration



The 5620 SAM supports the following HVPLS interconnectivity using spoke SDPs:

- VPLS to VPLS
- intra-VPLS
- VPLS to VLL

MVPLS

VPLS topology loops can occur if either of the following is true:

- Two VPLS are connected by redundant spoke SDPs.
- A CE NE is connected to a VPLS with redundant L2 access interfaces.

To remove topology loops, RSTP must be enabled on the redundant spoke SDPs or L2 access interfaces to block some of them from passing traffic. This requires the creation of an MVPLS.

MSTP is an extension of RSTP which allows VLANs to be grouped into spanning tree instances. Each instance has an independent spanning tree topology. MSTP can be run in an MVPLS to provide multiple forwarding paths for data traffic, which allows load balancing and reduces the number of spanning tree instances required to support a large number of VLANs. An MST region comprises a set of interconnected switches that have the same MST configuration. Each region can be configured with up to 16 MST instances. The instance with ID 0 is an internal spanning tree that runs an MST region and sends and receives BPDUs. All other spanning tree instance information is encapsulated within MSTP BPDUs.

An MVPLS is created to run RSTP or MSTP and manage traffic on the associated VPLS. An MVPLS contains sites, spoke SDP bindings, mesh SDP bindings, and L2 access interfaces. The MVPLS spoke SDP bindings and L2 access interfaces are configured to manage the associated VPLS spoke SDP bindings and L2 access interfaces.

In the case of spoke redundancy, the MVPLS runs RSTP on the redundant spoke SDPs and associates the resultant traffic-blocking actions with all VPLS that use the same spoke SDPs.

MVPLS traffic blocking can also be used on the access side to manage redundant L2 access interface connections. A VLAN ID range is specified for each MVPLS L2 access interface which identifies the VC IDs of the managed VPLS L2 access interfaces.

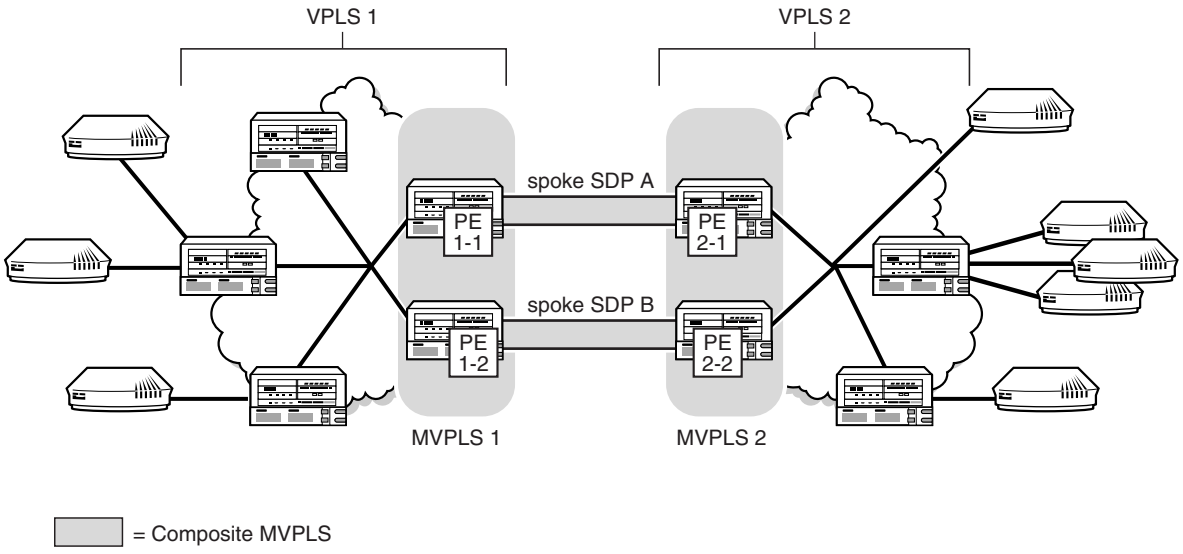
RSTP is enabled by default on an MVPLS. When the Admin state of an MVPLS is down, all managed L2 access interfaces and spoke SDPs in the associated VPLS are disabled. However, if the Admin state of individual L2 access interfaces or spoke SDPs of an MVPLS are down, then the managed VPLS L2 access interfaces or spoke SDPs are not affected by traffic blocking.

A common MVPLS situation occurs when two VPLS are connected by redundant spoke SDPs. If traffic is not blocked on one of the redundant spoke SDPs, then a loop results. To remove the loop, RSTP must be run on the spoke SDPs that form the loop to block one of the redundant spoke SDPs. Blocking is accomplished by creating an MVPLS on each side of the redundant spoke SDPs and creating a composite MVPLS to connect the MVPLS.

Another common MVPLS situation occurs when an access switch with many VLANs is redundantly connected to two other bridges, on which each uplink carries half the VLANs. MSTP allows you to build multiple spanning trees over VLAN trunks and to group and associate the VLANs to spanning tree instances, each with a different port instance cost and port instance priority.

Figure 68-2 shows an example of a composite MVPLS that is composed of MVPLS 1, MVPLS 2, and spoke SDPs.

Figure 68-2 Composite MVPLS



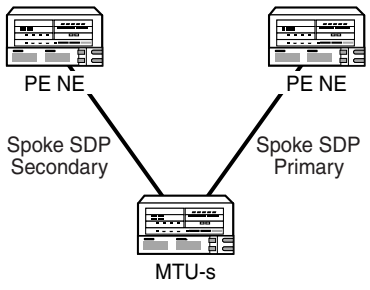
Another scenario occurs when multiple L2 access interfaces from a VPLS are connected to the same customer edge equipment. In this case, a single MVPLS must be created with L2 access interfaces defined to manage the traffic on the associated VPLS redundant L2 access interfaces.

Dual homing for VPLS

A VPLS can be configured for dual homing through the use of redundant spoke SDPs. 5620 SAM handles the redundant spoke SDPs by grouping them together to form an endpoint object. The redundant spoke SDPs provide active and standby pseudowires for the service. This spoke SDP access arrangement allows data flow control and management support without requiring STP, which cannot be enabled on a spoke SDP binding that is under an endpoint. For VPLS, you can associate only spoke SDP bindings with an endpoint, and each endpoint can be associated with a maximum of two spoke SDP bindings.

Figure 68-3 shows a simple dual homing configuration.

Figure 68-3 MTU redundant access to VPLS



VPLS dual homing provides the ability to have an NE deployed as an MTU-s with links to multiple PE NEs without requiring an MVPLS.

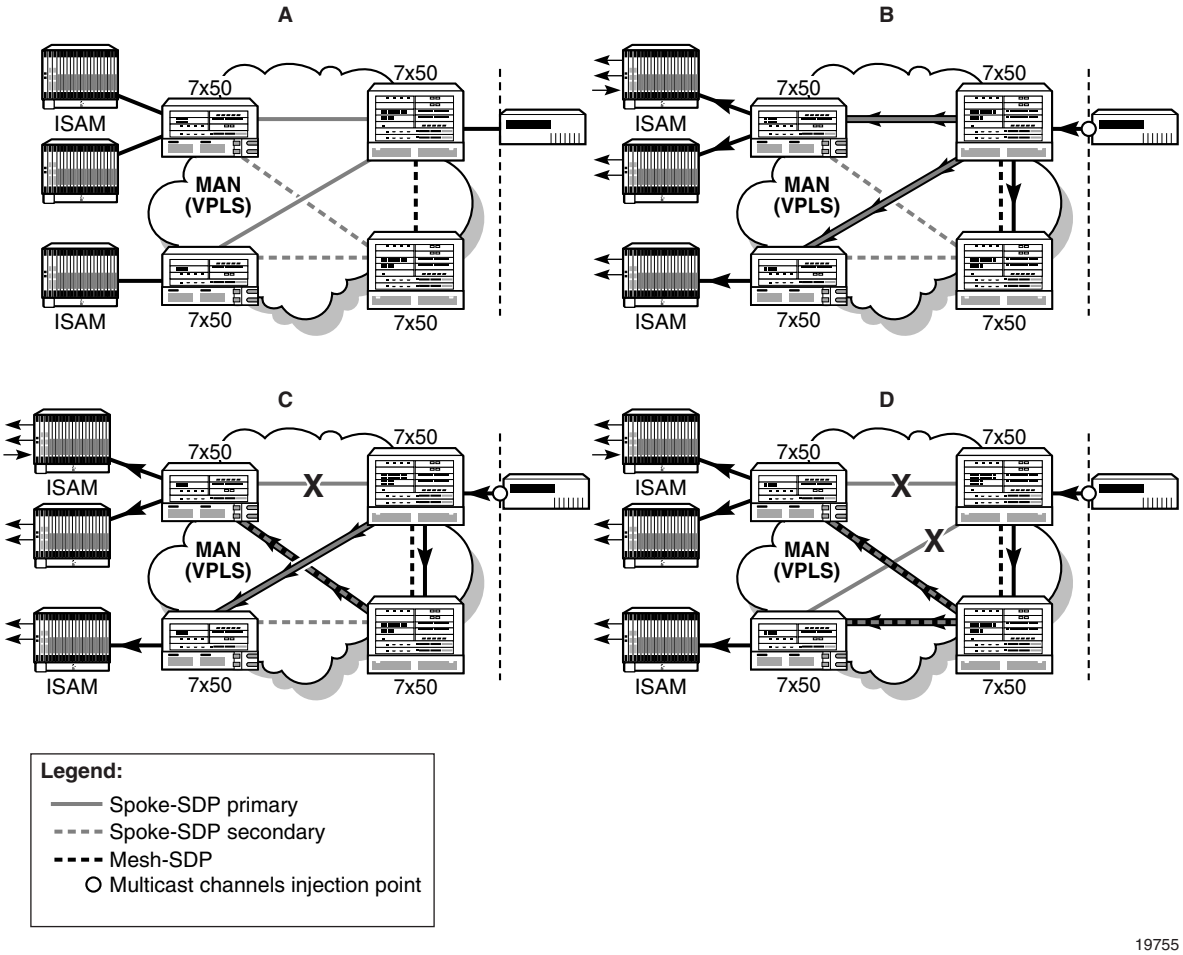
Note 1 — You cannot create a VPLS endpoint on a site that has an active or inactive MC ring SAP. See chapter 41 for more information.

Note 2 — You cannot create an endpoint in an MVPLS.

In this example, the MTU-s has spoke SDPs to two PE devices. One is designated as the primary spoke and the other as the secondary, or standby spoke, based on a precedence value specified for each spoke. The standby spoke is in a blocking state when the primary spoke is available. If the primary spoke becomes unavailable, the MTU-s immediately switches the traffic to the standby spoke. You can configure the service to revert back to the original configuration, after a specified delay, when the primary spoke is again available. Forced manual switchover is also supported.

You can configure a MAC flush to speed the convergence during a switchover. The PE devices that receive the MAC flush remove each MAC address that is associated with the affected VPLS instance and forward the MAC flush to the other PE devices in the VPLS. Figure 68-4 shows a dual-homed VPLS for BTV distribution.

Figure 68-4 BTV distribution in redundant VPLS architecture

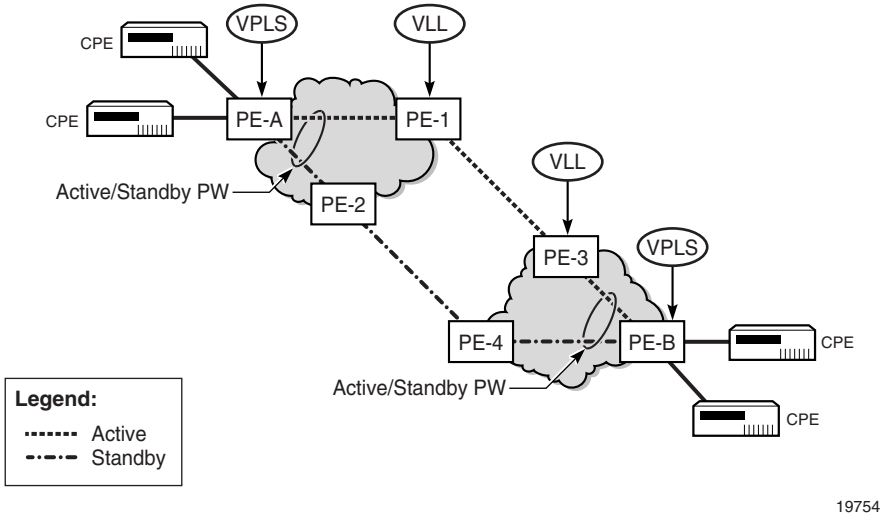


In the nominal operating mode shown in panel A, the edge router (grey icon) has been configured to statically join all multicast channels and inject them into the aggregation network. The access layer 7x50 unit (directly connected to ISAM) is dual-homed into two aggregation layer 7x50s edge routers (larger icons) using primary and secondary spoke SDPs. A mesh SDP interconnects both aggregation nodes. Injected BTV traffic from the edge router is broadcast on the primary spoke SDPs to the connected MTU devices (panel B).

A copy of the channels is also sent on the mesh SDP to the peer aggregation node, which also replicates the traffic to the connected spoke SDPs (aggregation layer nodes are not aware of primary/secondary spoke selection done by the MTU layer devices). The MTUs only receive traffic from the primary spoke SDP. Traffic received on the secondary spoke SDP is blocked. In the event of a link failure (panel C) or MDA failure (panel D), the MTU switches over to the secondary spoke SDP and immediately start receiving traffic from it instead of the primary spoke SDP.

Composite services also support VPLS with redundant spoke SDP bindings to VLL services. Figure 68-5 shows a VPLS and VLL combination example that provides an E2E redundant path.

Figure 68-5 VPLS and VLL combination to provide E2E redundant path



Provider Backbone Bridging in VPLS

Provider Backbone Bridging (PBB) is a technology configuration employed in next-generation networks that utilize carrier-grade Ethernet as the transport architecture. It addresses the potentially enormous increase in MAC addresses stored in the router lookup databases by encapsulating the customer frame in a Provider Ethernet header. The Customer MAC address (C-MAC) is then only dealt with by lower tier (or satellite) H-VPLS PEs. The core H-VPLS PEs only need to handle the MAC addresses (B-MAC) of the backbone provider, which are substantially less in number. For this reason, the technique is also referred to as MAC-in-MAC encapsulation.

IEEE 802.1ah defines an architecture and bridge protocols for interconnection of multiple Provider Bridge Networks (PBNs). PBB is defined in IEEE as a connectionless technology based on multipoint VLAN tunnels. MSTP is used as the core control plane for loop avoidance and load balancing. As a result, the coverage of the solution is limited by STP scale in the core of large service provider networks.

A Provider Backbone Bridged Network is a Virtual Bridged Local Area Network that comprises Backbone Edge Bridges (BEBs) and Backbone Core Bridges (BCBs) under the administrative control of a single backbone provider. Each BEB provides interfaces that encapsulate or verify the encapsulation of customer frames, and then relay those frames across the backbone. The term that the customer used may also mean a provider who is purchasing a service from another provider and using either a PBN or PBBN internally.

Backbone VLANs are used to create multipoint trunks in the backbone. The B-VLAN determines the route the frames take and limits broadcasting within the backbone. The B-TAG is added to the frame at the Customer Backbone Port (CBP). The selection of B-VLAN used to form the B-TAG is determined by the configuration of the CBP service instance table. This table maps ISIDs to B-VIDs and is created as part of service provisioning.

Backbone VLAN Connectivity

The backbone provider can use and configure MSTP to provide a number of independent spanning tree active topologies and can assign each B-VLAN to one of these active topologies to best use the resources in the network. MVRP, running in the context of each spanning tree active topology, configures the extent of each B-VLAN to the subset of that active topology necessary to support connectivity between the customer points of attachment to the instance of MAC service provided, and can reconfigure that connectivity as required if the spanning tree active topology changes. The operation of MSTP within a backbone provider's network is independent of the operation of any spanning tree protocol within attached provider or customer networks. This is achieved by removing all MSTP BPDUs received or to be transmitted at the service access interfaces. The operation of MVRP within a PBBN is independent of the operation of any configuration protocol within attached customer networks.

SR PBB implementation

The IEEE PBB model is organized around a B-component handling the provider backbone layer and an I-component concerned with the mapping of Customer/Provider Bridge (QinQ) domain (that is, MACs, and VLANs) to the provider backbone (that is, B-MACs, and B-VLANs). The I-component contains the boundary between the customer and backbone MAC domains. PBB encapsulates the customer payload in a provider backbone Ethernet header, which allows the C-MACs to be hidden from the core PEs. A special Group MAC is used for the Backbone Destination MAC when the customer frame type is either unicast, multicast, broadcast, or unknown.

The SR PBB solution can be summarized as follows:

- Two VPLS variants are employed, namely B-VPLS and I-VPLS, functioning as the B-type BEB, and the I-type BEB respectively. A B-VPLS instance (a service instance within a service router) and its corresponding I-VPLS instances must be co-located in a service router. From a network-wide perspective, a B-VPLS comprises multiple Backbone Virtual Switch Instances (B-VSIs).

  Note — For the description in this section and in the procedures in this chapter, B-VSI is used for a single B-type BEB instance, and is referred to as a B-Site. Similarly, I-VSI is used for a single I-type BEB instance, and is referred to as an I-Site.

- mB-VPLS and mI-VPLS are also available to provide loop avoidance for B- and I-VPLS in the same way as m-VPLS and regular VPLSs operate.
- A 5620 SAM VPLS can include regular sites and either B-Sites or I-Sites. The service should not contain both B-Sites and I-Sites. When a VPLS has at least one B-Site it becomes a B-VPLS. When a VPLS has at least one I-Site, it becomes an I-VPLS.

  Note — Regular sites, B-Sites, and I-Sites cannot change their type after they are created.

- An I-Site can be bound to one B-Site, but a B-Site can be used by multiple I-VPLSs.
- PBB is configurable on the 7450 ESS, 7710 SR, 7750 SR, 7950 XRS, OS 9700E, and OS 9800E.

B-VPLS and I-VPLS instances

PBB processing may be seen as a chain of two linked VPLS contexts, namely B-VPLS and I-VPLS. Their characteristics are summarized in the sections that follow.

I-VPLS

I-VPLS is the abbreviated form for Service Instance ID (ISID) VPLS. An I-VPLS instance on a service site is referred to as an I-Site.

The following are I-VPLS and I-Site characteristics:

- An I-Site operates using customer addressing and maps the C-MACs to B-MACs.
- You can select one B-Site to associate with an I-Site; the B-Site must be on the same PE NE as the I-Site.
- I-Sites support only spoke SDP bindings and not mesh SDP bindings.
- An I-Site L2 access interface, or I-SAP, can co-exist on a port with regular L2 access interfaces or subscriber management M-L2 access interfaces. The existing port encapsulation is supported. An encapsulation tag that is used for service selection on an I-SAP is removed before the PBB encapsulation is added. The appropriate encapsulation tags are added at the remote PBB PE when sending the packet out on the egress access interface.

- An I-Site can be connected to one or more regular VPLS sites. A regular (network level) VPLS can have a mix of regular sites and I-Sites. The I-Sites of such services are responsible for the mapping of C-MACs to B-MACs. The regular sites of the service function as normal (bridge).
- ISID is a 24-bit field that carries the service instance identifier associated with this frame. It is used at the destination PE as a demultiplexer field, a function similar to a VC label. Default to service ID only works if the service ID is within the ISID range. For a service with service ID larger than 16 777 215, the ISID value must be specified.
- The ISID must be unique on one router.
- The Provider MSTP support in an M-VPLS is in the I-VPLS space.
- The I-Site MTU must be at least 18 bytes smaller than the B-Site MTU to which it is bound.
- If a VPLS has an attached I-Site, the Include I-Site(s) indicator on the General tab of the VPLS configuration form is selected.
- IGMP snooping can be configured for I-Sites and I-L2 Access Interfaces, except on routed I-VPLS services.

Backbone-VPLS (B-VPLS)

Multiple L2 services can use a single B-VPLS. Ordinarily, a pair of SDP bindings (in opposite directions) provide either point-to-point connection between two sites of a service (as SDP bindings) or between different services (as a service connector). However, a B-VPLS provides a multipoint connection between sites of a service or for multiple services.

The following are properties and characteristics of a B-VPLS and B-Sites:

- The B-VPLS operates using the provider or backbone addressing (B-MACs).
- The B-VPLS provides backbone tunneling for one or multiple I-VPLSs.
- The B-VPLS accepts mesh or spoke SDP bindings, thereby providing both routing and MAC hiding using PBB/PW encapsulation.
- The B-VPLS accepts access interfaces using PBB encapsulation for tunneling through an Ethernet-only network.
- A regular (network level) VPLS can have a mix of regular sites and B-Sites to function as a B-VPLS (that is, operating using B-MACs).
- The backbone's Source MAC address can be configured on a B-Site. All the I-Sites provisioned under this B-Site shares the provisioned values. By default, this is a loopback chassis MAC address. It must be a unicast MAC address.
- A B-Site site can not be deleted until all its I-Site associations are removed.
- A B-Site can have both spoke and mesh SDP bindings and only an MPLS type of tunnel can be used (including LDP SDP). This also applies for a regular pseudowire, where the outgoing PBB frame on a B-SDP (that is, a B-PW) contains a B-VID qtag only if the PW type is Ethernet VLAN. Alternatively, if the pseudowire type is Ethernet, the B-VID qtag is stripped before the frame goes out.

- Only Null, dot1q, and QinQ encapsulation types can be used by a B-Site L2 access interface. These access interfaces must use PBB encapsulation and have the following properties:
  - Ethernet dot1q is applicable to the bulk of PBB use cases, such as one B-VID.
  - Ethernet Null is supported for direct connection between neighboring I-VPLS, for example, when no B-VID is required and all traffic is sent to or from local I-VPLS.
  - There is no requirement for a PBB SAP type for PBB on the B-VPLS SAPs. Only the B-VID is used for tunnel delimitation on the port.
  - The default access interface type is blocked for the B-L2 access interface.
  - The following rules apply to the SAP processing of PBB frames:

    > For transit frames (frames not destined to a local MAC), there is no need to process the I-tag component of the PBB frames. Regular Ethernet SAP processing is applied to the backbone header (B-MACs and B-VID).

    > If a local I-VPLS instance is associated with the B-VPLS, then local frames (frames originated or terminated on local I-VPLSs) are PBB encapsulated and de-encapsulated using the pbb-etype provisioned under:

    related port->I-VPLS->root pbb component

    (listed in decreasing order of precedence, where the related port is highest in the order).
- If a VPLS has an attached B-Site, the Include B-Site(s) indicator on the General tab of the VPLS configuration form is selected

Service topology map views

Service and composite service topology maps support PBB.

The service map shows different types of sites with various icons for I-Sites, B-Sites, and Epipe PBB sites. With an I-VPLS bound to B-VPLS, the map shows the PBB backbone network as a cloud. The bindings between I-VPLS and B-VPLS are shown as a binding link.

MRP and MMRP support

The Multiple Registration Protocol allows participants in an MRP application to register Group MAC addresses with other participants in a Bridged LAN. An MRP participant may transmit and receive MRP PDUs. For the PBB implementation, the MRP parameters can be configured at the service site level, on the access interface, or the SDP binding.

If MRP is enabled on the NE, the 5620 SAM MMRP application automatically advertises the presence of the Group B-MAC address on the active B-VPLS virtual links—that is, on the B-Site spoke bindings or the B-L2 access interfaces. You can view the MMRP entries advertised and/or received on the Forwarding Control→MMRP Entries tabs of the B-Site spoke bindings or the B-L2 access interfaces. All of the MMRP entries may also be viewed together at the I-Site level.

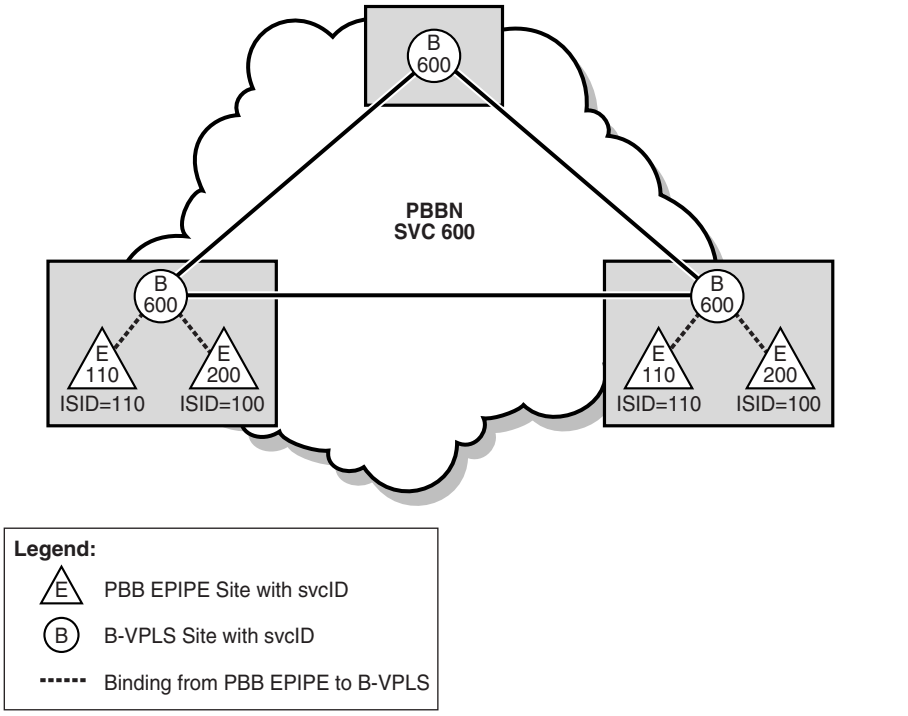
Epipe service with PBB

A PBB tunnel may be linked to an Epipe and to a B-VPLS. MAC switching and learning is not required for the point-to-point service, since all packets ingressing the Epipe access interface are PBB encapsulated and then forwarded to the PBB tunnel for the backbone destination MAC address. Similarly, all the packets ingressing the B-VPLS and destined for the ISID are PBB de-encapsulated and then forwarded to

the Epipe access interface. A fully-specified backbone destination address must be provisioned for each PBB Epipe instance to be used for each incoming frame on the related Epipe L2 access interface. If the backbone destination address is not found in the B-VPLS forwarding database, then packets may be flooded through the B-VPLSs.

To enable an Epipe service with PBB, the Epipe site is configured as a PBB site and functions similarly to a VPLS I-Site. This can only be specified during the site's creation. On the Epipe PBB site, you select a B-Site that acts as the tunnel for the Epipe. You also specify the destination B-MAC address of the remote PE where the other site is located. Figure 68-6 shows a simplified view of this configuration.

Figure 68-6 Epipe service link to a B-VPLS



See the *7750 SR OS Services Guide* for more information about PBB.

SPB in VPLS

SPB simplifies network creation and configuration because service provisioning is required only at the network edge. SPB uses IS-IS to dynamically build the topology between NEs. The 5620 SAM supports SPB on B-VPLS services.

SPB allows shortest path forwarding in a mesh network by using multiple equal cost paths. In addition, SPB supports a link state spanning tree. SPB is appropriate for larger layer 2 topologies, with faster convergence than STP variant protocols for the same size networks, and improved use of the mesh topology.

The main components of B-VPLS SPB are:

- control B-VPLS
- user B-VPLS

The control B-VPLS defines the SPB IS-IS instance and is associated with an ECT algorithm and a set of SAPs or spoke SDPs for link connectivity. The user B-VPLS is a logical B-VPLS subset of the control B-VPLS. User B-VPLSs are associated with the forwarding ID, which is a logical backbone VLAN ID, that you define in the control B-VPLS. The user B-VPLS forwarding ID does not have to match the control B-VPLS forwarding ID. The user B-VPLS must be a subset of the control B-VPLS, or else a black hole can occur.

Control and user B-VPLS SAPs and SDP bindings are fate-shared. You must configure these SAPs and SDP bindings to use the same links and resources. SAPs and spoke SDP bindings that do not use the same links and resources (non-fate-shared) can exist in the user B-VPLS configuration but do not carry traffic.

Consider the following when you enable SPB on a B-VPLS:

- B-VPLS mesh SDP bindings are not supported in control or user SPB B-VPLSs.
- STP can be configured but not enabled.
- two Dot1Q SAPs on the same physical port cannot exist in a user or control SPB B-VPLS.
- Two QinQ SAPs with same top bit on the same physical port cannot exist in a user or control SPB B-VPLS.
- Control or user SPB B-VPLS SAPs cannot exist on physical ports that are managed by MSTP.
- MVPLSs and SPB B-VPLSs cannot share the same spoke SDP tunnel.
- .0 and 0.* SAPs cannot exist on a user or control SPB B-VPLS.
- SPB B-VPLS services that support multiple I-VPLSs do not share forwarding IDs. A B-VPLS that has I-VPLS services must have a different forwarding ID.
- A control SPB B-VPLS can be associated with none or many user SPB B-VPLSs.
- A user SPB B-VPLS must be associated with a control SPB B-VPLS.
- MVPLS and SPB B-VPLS cannot share the same spoke SDP tunnel.
- SHG is not supported.
- G803.1 tunnels are not supported.
- G.8032 access is not supported.

You can perform the following OAM diagnostic tests on SPB-enabled B-VPLSs:

- CFM link trace
- CFM loopback



Note — SPB does not support MEPs on SAPs and spoke SDP bindings. You cannot create an SPB instance on a control or user B-VPLS if any MEPs or MIPs are enabled on a SAP or spoke SDP binding. Virtual MEPs are supported. You cannot configure MIPs on SPB-enabled SAP and spoke SDP bindings.

Static B-MACs and ISIDs

An SPB interface on a SAP or SDP can have static B-MACs and static ISIDs that are not part of the SPB network or region. Static B-MACs and ISIDs allow SPB networks to interface with other PBB networks that use other control planes. Static B-MACs allow remote PBB Epipes to connect to SPB managed networks. Static ISIDs allow I-VPLS services to connect to non-SPB I-VPLS services. You can define an ISID policy to use the default multicast tree and to suppress the advertisement of ISIDs in SPB when I-VPLS or static ISIDs are used for unicast services. See Procedures 68-67, 68-68, and 68-69 for more information.

SPB B-VPLS audit

You can perform an RCA audit on an SPB-enabled B-VPLS to verify whether:

- all user B-VPLS SAPs and spoke SDP bindings are fate-shared with a control B-VPLS. The following are the fate-sharing rules:
  - a user B-VPLS Dot1Q SAP fate-shares with the control B-VPLS SAP if they are in the same physical port
  - a user B-VPLS QinQ SAP fate-shares with a control B-VPLS SAP if they are in the same physical port and have the same top tag
  - a user B-VPLS spoke SDP binding fate-shares with a control B-VPLS spoke SDP binding if they are in the same SDP
- user B-VPLS instances belonging to the same service on different sites must have same forwarding ID
- the ECT-to-forwarding ID mapping is consistent on all the sites for the active B-VPLS services
- the ISID policy (Control/User) of all sites in the B-VPLS is consistent. All sites in this service must have the same ISID configuration if the Use Default Multicast Tree and No Advertise Local parameters are enabled.
- the ISID policy (Control/User) of all sites in the B-VPLS is configured. ISID ranges that are defined by one service site are be defined by all service sites of this service.

See chapter 80 for more information about the SPB B-VPLS RCA audit.

BGP Auto Discovery

BGP Auto Discovery enables a VPLS PE router to discover other PE routers that are part of the same VPLS domain. This allows each PE's configuration to consist only of the identity of the VPLS instance established on a specific PE, and not the identity of every other PE in that VPLS instance. If you need to change the VPLS topology, only the affected PE's configuration needs to change. Other PEs automatically discover the change using MP-BGP and adapt themselves accordingly. In contrast, if the BGP AD functionality is not used, you must then explicitly configure each PE router with the identities of all the other PEs in a specific VPLS.

You must assign a single, globally unique VPLS-ID to each VPLS (that is, the same value for all sites to the same VPLS across the entire network). The VPLS-ID eliminates the possibility of a collision between VPLSs belonging to different service providers.

There is also a globally unique Route Distinguisher (RD) ID associated with a VPLS. Each site also needs a unique ID that is a BGP NLRI. The PE address does not have to be globally routable, but it must be unique within the VPLS. The PE ID can be the PE router ID, for operational convenience.

Each site must also be associated with one or more RT Extended Communities, and the RTs control the distribution of NLRIs.

Each PE distributes the NLRI for each of its sites, with itself as the BGP next hop, and with the appropriate RT for each NLRI. A PE with a specific RT imports all NLRIs that have that same RT (and learns the other PEs addresses through their next hops). H-VPLS can be configured by using multiple RTs.

In summary, the BGP advertisement for a specific site in a PE includes:

- An NLRI. This is the VSI-ID.
- A BGP next hop equal to the loopback address of the PE.
- An extended community attribute containing the VPLS-ID.
- An extended community attribute containing one or more RTs.

Targeted-LDP [(T-)LDP] signaling is set up for the point-to-point PWs between sites using the selected (T-)LDP sessions corresponding to the remote PE(s) that have been recently added to their list.

To auto-create a spoke SDP binding, you must create a PW template policy and distribute the policy to the NEs. The 5620 SAM policy distribution mechanism is used to send out the template and maintain consistency in the network. The template selection is at the PE level, not at the service level, because not all PEs are capable of supporting BGP AD and some VPLS sites may not support BGP discovery.

Consider the following with regard to tunnel creation:

- If you plan to use BGP AD for all or part of the VPLS, you must not enable automatic mesh SDP binding creation.
- A provisioned PW to a specific remote PE takes precedence over one that is auto-discovered using BGP AD. In other words, if there is an existing SDP binding available, the router selects this existing binding and does not automatically create a new one.
- When the 5620 SAM auto-tunnel creation function is being used for non-BGP AD VPLSs, the automatically-created components are excluded from discovery. Also, you cannot select an automatically-created SDP or SDP binding when you create a service tunnel that is to be used as part of a BGP AD VPLS.

A 5620 SAM-managed VPLS or H-VPLS may consist of various site types located on different PEs, and which in turn, may be of differing versions. Due to these possibilities, some restrictions apply in terms of using Auto Discovery. For example, an M-VPLS site cannot be in the same service with a regular site. However, BGP AD-enabled sites and regular sites can be components of the same VPLS.

BGP VPLS

BGP VPLS is an extension of the VPLS concept. When configured as a BGP VPLS, such a service can interconnect with another BGP VPLS across different VPLS domains.

The control plane of the BGP VPLS provides auto-discovery and signaling capability. In this context, auto-discovery is a means for a PE router to discover other remote PE routers that are members of a given VPLS. The signaling function enables a PE router to know which pseudowire label a given remote PE router will use when sending the data to the local PE router. The BGP VPLS control plane carries sufficient information to provide the auto-discovery and signaling functions concurrently.

Some of the major features of the Alcatel-Lucent BGP VPLS solution include:

- The data plane is identical with the BGP AD (LDP VPLS) solution. For example, VPLS instances are interconnected via a pseudowire mesh. Split horizon groups may be used for loop avoidance between the pseudowires.
- Addressing is based on a two-byte VE ID assigned to the VPLS instance.
- The target VPLS instance is identified by the Route Target (RT) contained in the MP-BGP advertisement (extended community attribute).
- Auto-discovery is MP-BGP based.
- Pseudowire label signaling is MP-BGP based. As a result, the BGP NLRI content also includes label related information such as block offset, block size, label base, and so forth,

The Alcatel-Lucent BGP VPLS solution is compliant with RFC 4761.

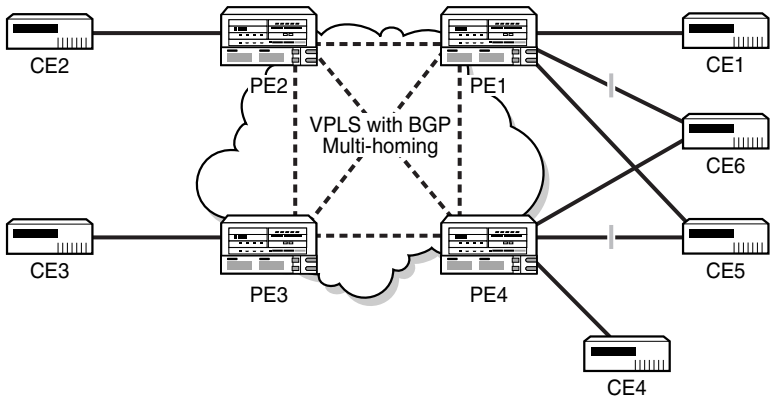
See the *7750 SR OS Services Guide* for more information regarding BGP VPLS.

BGP VPLS Multi-homing

The 5620 SAM allows BGP VPLS multi-homing to be established for CEs and access PEs by first configuring the multi-homing VPLS sites and then assigning the same multi-homing site ID to each.

Figure 68-7 shows an example of this approach, where a VPLS contains certain CEs that are multi-homed to pairs of VPLS PEs.

Figure 68-7 CE Multi-homing in VPLS



The BGP/LDP-signaled PW infrastructure (shown as the cloud at the center) is used to interconnect the VSIs between PEs. In this example, CE5 and CE6 are dual-homed to PE1 and PE4. To avoid loops, only one SAP must be active at any point in time between any multi-homed CE (such as CE5 or CE6) and its pair of connected PEs (such as PE1 and PE4). The others are blocked. Service providers use their MP-BGP on PE1 and PE4 to control the activation of the SAPs connected to the same customer site.

Other CE topologies (for instance, square connectivity) where, for example, CE1 and CE4 are part of the same customer site (and are themselves interconnected) are also supported.

When multi-homing a VPLS site using BGP (potentially into different autonomous systems), the PE routers (for example, PE1 and PE4) that are connected to the same customer site (for example, CE5) are configured with the same multi-homing ID. In this way, a loop-free topology is constructed using a routing mechanism such as BGP path selection. When a BGP speaker receives two equivalent NLRIs, it applies standard path selection criteria such as local preference and AS path length to determine which NLRI to choose.

Two VPLS NLRIs are considered equivalent from a path selection perspective if the following are identical:

- Route distinguisher
- Multi-homing ID

MVR on VPLS

MVR on VPLS is a bandwidth optimization method for applications on a broadband services network. At the port level, MVR allows a VPLS end user to subscribe or unsubscribe to a multicast stream on one or more network-wide multicast VPLS instances without requiring that the stream be part of the customer VPLS.

MVR on VPLS is a mechanism through which the supporting devices are able to participate in a multicast distribution system. Separate, dedicated VLANs must be constructed specifically for multicast traffic distribution.

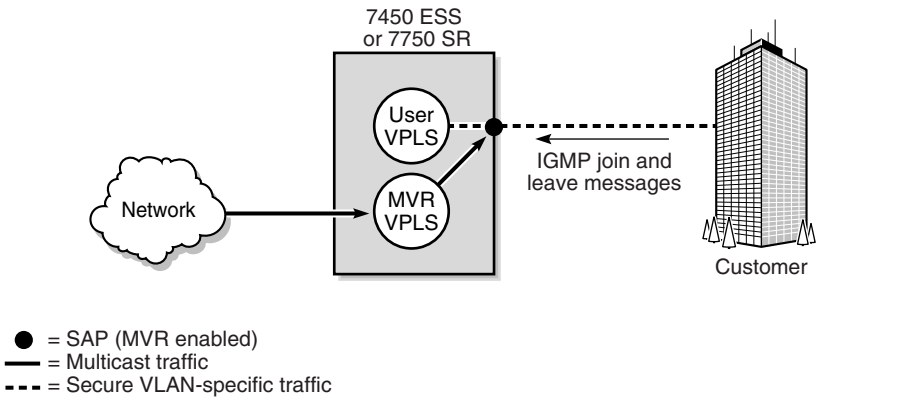
MVR assumes that hosts join and leave multicast streams by sending IGMP join and leave messages. The IGMP join and leave messages are sent inside the VPLS to which the host port is assigned. The multicast VPLS is shared in the network while the hosts remain in separate VLANs. For example, two user VPLS that are bound to the same MVR VPLS cannot exchange any information, but the same multicast service can still be provided to them.

An MVR VPLS is a VPLS that is responsible for sending multicast traffic through the network. An MVR VPLS is associated with a multicast package policy and has MVR-enabled sites. The MVR VPLS is configured to distribute certain multicast streams. An MVR VPLS can also be configured as a user VPLS to receive multicast traffic.

A user VPLS is a VPLS that contains SAPs that can receive multicast traffic from an MVR VPLS. Each SAP must be configured individually to use a specific MVR VPLS. Any VPLS, including an MVR VPLS, can be used as a multicast receiver for an MVR VPLS. IGMP and/or MLD snooping must be enabled on each site.

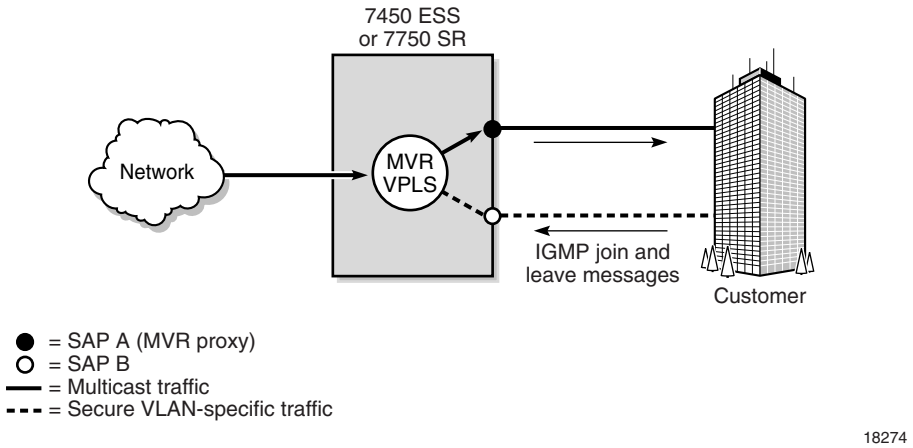
Figure 68-8 shows an example of MVR on VPLS. MVR reacts only to join and leave IGMP messages from the multicast groups configured for the MVR VPLS with which the user VPLS is associated. Join and leave messages from all other multicast groups are managed by IGMP and/or MLD snooping. Therefore, several MVR VPLS instances can be configured, each with its own set of multicast channels.

Figure 68-8 MVR on VPLS



In some situations, such as when a host is connected to a 7301 ASAM, the multicast traffic cannot be sent from the MVR VPLS to the VLAN on which the IGMP message was received (standard MVR behavior) but to another VLAN. This configuration is known as MVR by proxy. The 7450 ESS, 7750 SR, 7710 SR, and 7950 XRS allow multicast traffic to be sent to a SAP other than the SAP from which the IGMP message originated. When configuring MVR by proxy, you must indicate the MVR VPLS on which the multicast channel is available and the SAP to which the multicast traffic must be copied. Figure 68-9 shows an example of MVR by proxy.

Figure 68-9 MVR by proxy



Configuring MVR on VPLS using the 5620 SAM involves the following steps.

1 Configure PIM before configuring MVR. See chapter 23 for more information.

2 Create a multicast package policy for all supporting NEs in an MVR VPLS. See chapter 45 for more information.

   Alternatively, you can configure NEs individually in an MVR VPLS using a routing policy. See Procedure 22-15 for more information.

3 Create the MVR VPLS. See Procedure 68-17 for more information.

   - Associate the multicast package policy with the service, which indicates that a VPLS is an MVR VPLS.
   - Specify the VPLS sites that are the sources of the multicast groups. MVR must be enabled on each site.
   - Configure SAPs only if you are configuring the MVR VPLS to be a user VPLS as well. See Procedure 68-1 for more information about configuring a user VPLS.

4 Create the user VPLS. See Procedure 68-1 for more information.

   - The SAPs are standard host access points.
   - Configure IGMP and/or MLD snooping and MVR on each site.
   - Associate the MVR VPLS with each SAP for which access to multicast traffic is needed. This association means that IGMP requests received at that SAP for a multicast group are fulfilled as long as the multicast group being requested is included in the multicast package policy of the MVR VPLS. After the SAPs in a user VPLS have been associated with a specific MVR VPLS, the SAP becomes known to the MVR VPLS.

5 If using MVR by proxy, configure a VPLS SAP that is to act as the MVR proxy. See Procedure 68-17 for more information.

In a situation in which an MVR VPLS has VPLS sites that do not support MVR, the following conditions apply.

- The ability to configure MVR is not available for the VPLS sites and SAPs of a device that does not support MVR.
- Multicast package policies are not distributed to the devices that do not support MVR.

GSMP group on VPLS

The edge devices determine the circuit that opens an ANCP session. ANCP provides status and control information such as current line rate and port-up and port-down messages to the edge devices. The edge devices perform the following functions:

- adjust the H-QoS subscriber scheduler with the correct rate
- raise an alarm when the rate goes below a set threshold
- send DSL line OAM commands to complete OAM tests

A GSMP group is created under the GSMP tab of the VPLS site form. Multiple groups can be defined and different ANCP capabilities can be associated with different groups. A neighbor can be defined in a GSMP group. Multiple neighbors can be configured for each group.



Note — A GSMP group must be configured on VPLS, MVPLS or VPRN for an ANCP session to open.

L2 management interfaces on VPLS

L2 management interfaces act as a host. L2 management interfaces are created the same way out-of-band interfaces are created on VPLS. L2 management interfaces are used for CPM protocols such as telnet, SSH, SNMP, ping, and ANCP.

CPM filtering is used to limit access to L2 management interfaces.

Routed VPLS

A routed VPLS connector joins an L3 access interface within an IES or VPRN service context to a VPLS service on the same site. When an IES or VPRN IP interface is bound to a VPLS site name, the site name cannot be bound to another IP interface. While an IES or VPRN IP interface can only be bound to a single VPLS site, the service context containing the IP interface can have other IP interfaces bound to other VPLS sites. Both the IES or VPRN IP interface and VPLS site must be located on the same NE.

If a VPLS site name does not exist within the system, the binding between the IP interface and the VPLS site remains operationally down until a VPLS site name is assigned to the VPLS site. When an IP interface is bound to a VPLS site, the operational state of the routed VPLS binding is dependent upon the operational state of the VPLS site, and whether the IP interface binding is enabled on the VPLS site.

This functionality is limited to supporting devices.



Note 1 — You can create and manage a routed VPLS connector from the navigation tree on the Composite Service (Edit) form or from an IES or VPRN access interface form, routed VPLS path.

Note 2 — The routed VPLS binding will not be operationally up until the Enable IP interface binding parameter is set to true and the VPLS site is operationally up. See Procedure 68-7 for more information.

Note 3 — You can add a routed VPLS L3 access interface to an IGMP interface on an IES or VPRN service.

FIBs

The FIB is the set of information that represents the best forwarding information for a destination. A FIB entry is analogous to a static MAC address, and every computer and network node has a MAC address that is hardware-encoded. In 5620 SAM, static MAC addresses can be also created on VPLS endpoint objects, access interfaces, and service circuits.

The edge devices perform the packet replication required for broadcast and multicast traffic across the bridged domain. Devices perform MAC-address learning to reduce the amount of unknown destination MAC address flooding. The edge devices learn the source MAC addresses of the traffic arriving on their access and network ports. You can also specify and manage static MAC addresses using the FIB entries table.

Each device maintains a FIB for each VPLS instance. Learned MAC addresses are populated in the FIB table of the service. All traffic is switched based on MAC addresses and forwarded between all participating sites using the service. Unknown destination packets (i.e., the destination MAC address has not been learned) are forwarded on all LSPs to the participating devices for that service until the router responds and the MAC address is learned by the device associated with that service.



Note — Each VPLS FIB entry consumes system resources. The devices allow you to set the maximum number of MAC entries allowed in a VPLS instance to prevent a VPLS instance from consuming a disproportionate amount of resources.

The size of the VPLS FIB can be configured with a low watermark and a high watermark expressed as a percentage of the total FIB size limit. If the actual FIB size grows above the configured high watermark percentage, an alarm is generated. If the FIB size falls below the configured low watermark percentage, the alarm is cleared.

MAC learning

Like an L2 device, learned MACs within a VPLS instance can be aged out if no packets are sourced from the MAC address for a specified period of time (the aging time). In each VPLS, there are independent aging timers for locally learned MAC and remotely learned MAC entries in the FIB. A local MAC address is a MAC address associated with an access interface, because it ingressed on a SAP. A remote MAC address is a MAC address received using a service tunnel from another device that is part of the VPLS.

Unknown MAC discard is a feature which discards all packets ingressing the service where the destination MAC address is not in the FIB. The normal behavior is to flood these packets to all end points in the service.

MAC learning can also occur for Split Horizon Groups (SHG) but with accompanying risks. For example, in an L2 environment of an SHG, hosts (among whom mutual communication is disallowed) can launch DoS attacks by sending a flood of packets that source an uplink MAC address to unprotected customer SAPs.

This situation can be managed by controlling MAC learning on SAPs and SDPs. When a frame arrives at a protected SAP or SDP, the MAC is applied to its learning table; when a frame arrives at an unprotected customer SAP or SAP containing the address of a protected source MAC address, the system can be configured to take one of the following actions:

- The frame is immediately dropped and not learned by the unprotected SAP. As a result, the unprotected SAP does not know the MAC address of the uplink and, therefore, cannot use it to flood packets to other SAPs in the SHG.
- The frame is not dropped, but an alarm is generated.
- The SAP is placed in an operational Down state.

In addition, you can specify automatic population of the MAC protect list with source MAC addresses learned on the SAP or SDP.

Auto Learn Mac Protect and Restrict Protected Source functionalities are supported on SAPs, spoke and mesh SDP bindings, split horizon groups, and endpoints under a VPLS service. The functionality is also supported on Service PW-Template policies, in order to allow its use with BGP auto discovery for spoke SDP bindings and split horizon groups.

MAC move

A sustained high MAC re-learn rate can be a sign of a loop somewhere in the VPLS topology. Typically, STP detects loops in the topology, but for those networks that do not run STP, the MAC move feature is an alternative way to protect the network against loops.

When enabled on a VPLS, MAC move monitors the re-learn rate of each MAC. If the rate exceeds the configured allowed limit, it disables the SAP on which the source MAC last arrived. The SAP can be disabled permanently or for a length of time that grows linearly with the number of times the SAP is disabled.

There is also the option of marking a SAP as non-blockable, which means that when the re-learn rate exceeds the limit, another SAP—one that is blockable—is disabled instead. When the MAC move parameter is set to blockable, ports can be blocked in a specific order depending on the number of times the re-learn rate exceeds the configured threshold period.

MAC move is configurable on VPLS SAPs and VPLS spoke SDPs. Blocking information for an object is displayed on the MAC move configuration form for the object. This information includes:

- the number of MAC learning retries that remain before blocking occurs
- the time that remains before the blocked object is unblocked
- the order of blocking, starting with tertiary, secondary and primary

Flooding

Traffic that is normally flooded throughout the VPLS can be rate limited on SAP ingress through the use of Service Ingress QoS Policies. In a Service Ingress QoS Policy, individual queues can be defined per forwarding class to provide shaping of broadcast traffic, MAC multicast traffic and unknown destination MAC traffic. You can also specify how to classify frames.

Multiple services and service types can be configured on a port. VPLS spanning tree protocols are configured on a per-service site basis, not a per-port basis, thus, multiple instances of STP per site are supported. Unknown destinations, broadcasts, and multicasts are flooded to all other SAPs in the service.

The flooding mechanism and the way that the Interior Gateway Protocol (IGP) operates ensure that no packets are duplicated on any interface. If SAPs are connected together, either through misconfiguration or for redundancy purposes, loops can form and duplicate packets can traverse the network. The STP is designed to prevent multiple SAPs from forwarding a packet into the VPLS

Spanning tree protocols

The 5620 SAM supports RSTP for VPLS instances and maintains support for legacy STP implementations. STP on the 7710 SR, 7750 SR, and 7950 XRS incorporates an optimized and compatible implementation of IEEE 802.1D which attempts to eliminate STP blocking of links in the core of the VPLS. STP on the 7210 SAS-M, 7210 SAS-T, and 7450 ESS is used to guarantee that service tunnels are not blocked in any circumstance while not imposing artificial restrictions on the placement of the root bridge in the network. To provide this support, all mesh service tunnels are configured as root ports or designated ports.

RSTP, which is the default STP mode managed by the 5620 SAM, is compliant with IEEE standard 802.1D-2004. Other available STP types include an RSTP variant with 802.1w-2001 backward compatibility, an STP variant that is compliant with 802.1w-2001, and MSTP, an STP variant that is compliant with 802.1s-2002. The following devices support MSTP:

- 7210 SAS-M
- 7210 SAS-T
- 7210 SAS-X
- 7450 ESS
- 7710 SR
- 7750 SR
- 7950 XRS

The 5620 SAM verifies STP parameters that are configured within each VPLS instance. However, it does not check the compatibility of STP configurations between interconnected VPLS instances.

IGMP snooping

IGMP snooping allows a device to snoop packets sent between IP multicast devices and IP multicast hosts to learn the IP multicast group membership. The device checks the IGMP packets for the group registration information, and configures multicasting accordingly.

Without IGMP snooping, multicast traffic is forwarded to all ports, which is the same as broadcast traffic. IGMP snooping ensures that multicast traffic is forwarded only to ports that are members of a specific multicast group to reduce the amount of multicast traffic that passes through the device.

You can enable IGMP snooping for VPLS sites, access interfaces, and spoke SDPs. IGMP snooping is supported on the following devices:

- 7210 SAS
- 7450 ESS
- 7710 SR
- 7750 SR
- 7950 XRS
- OS 9700E and OS 9800E



Note — IGMP snooping is not supported when MAC subnetting is enabled.

MLD snooping

Multicast Listener Discovery snooping is essentially the IPv6 version of IGMP snooping. The guidelines and procedures are very similar to IGMP snooping.

When MLD snooping is not enabled, L2 switches treat multicast traffic like an unknown MAC address or broadcast frame, that is, the frame is flooded out on every port of a VLAN. When MLD snooping is enabled, switches snoop the frame's L3 header for more efficient switching. In the context of IP multicast, only hosts that have expressed interest in receiving packets for the multicast groups have the frames forwarded to them.

The 7x50 and 7710 SR routers allow the enabling of MLD snooping for VPLS. A database of group members (per VPLS instance) is built by listening to MLD queries and reports from each SAP and SDP of the instance. These reports are forwarded to the multicast routers, if any are present.

MLD snooping is not supported when MAC subnetting is enabled.

Consider the following:

- Multicast groups can be learned (using the destination IP addresses of multicast packets) through MLD snooping or by static configuration at the port.
- The Fast leave feature modifies the membership leave mechanism by terminating the session immediately, rather than issuing a group-specific query to check if other members are still present on the network. Therefore, if a port (SAP or SDP) is configured for Fast leave, the session is terminated immediately without checking if the port also has other hosts subscribed to that same multicast group.
- A multicast router retains a list of multicast group memberships for each attached network. Therefore, a multicast router can assume the role of querier or listener. However, there can be only one querier per physical network.
- MLD snooping statistics are collected for each NE port, SAP, or SDP binding, and are viewable from the Statistics tab of a VPLS site properties form.
- The 5620 SAM supports MLDv1 and MLDv2.
- The 5620 SAM supports MVR.
- MLD snooping can co-exist with IGMP snooping and PIM snooping.
- MAC-based forwarding entries can be built using MLD snooping results.

PIM snooping

Protocol Independent Multicast snooping for VPLS allows a VPLS PE router to build multicast states by snooping PIM protocol packets that are sent over the VPLS. The VPLS PE then forwards multicast traffic based on the multicast states.

When all receivers in a VPLS are IP multicast routers running PIM, multicast forwarding in the VPLS can be efficient when PIM snooping for VPLS is enabled. After PIM snooping is turned up at the service level, all sites have PIM snooping configured and are set to the down state, by default. If any site does not support this feature, the 5620 SAM treats it as having PIM snooping turned off.

Since PIM snooping operates on PIM Hello packets as well as Join/Prune packets, PIM neighbors of the current router are learned by snooping on Hello packets. Therefore, in a meshed VPLS, every node learns from every other node's Hello packet and considers that node as a neighbor.

VPLS PE routers only snoop on PIM Hello and Join/Prune packets; they do not generate PIM messages on their own. Therefore, when PIM snooping is configured at the service level, all CE routers must have Join/Prune suppression disabled. If a VPLS PE router detects a condition where Join/Prune suppression is not disabled on one or more CE routers, the PE router puts PIM snooping into a non-operational state for the entire service. A trap on the PE is generated to report this condition and an alarm is raised to the 5620 SAM operator. To bring PIM snooping back to the operational state, PIM snooping must be disabled and then re-enabled.

Since PIM uses state refreshes, VPLS PE routers may not learn multicast states from all the CE routers, if PIM snooping was just enabled or the all snooping state was just cleared, until the next refresh.

To avoid traffic interruption, PIM snooping should hold up its operations for a period of time (60 seconds, if default timer is used). During this period of time, multicast traffic is flooded in the VPLS just like snooping was not enabled. SAM should have this hold-up timer configurable on VPLS properties panel having range 0-120 with 60 secs as default.

A variety of statistics are gathered for PIM snooping operation and are available for viewing and analysis in the PIM Snooping tab of a VPLS configuration form under the Multicast tab.

PIM snooping is not supported when MAC subnetting is enabled.

PIM snooping only supports IPv4.

Split horizon groups

SHGs control traffic that flows through SAPs or spoke SDPs for a VPLS site. SHGs prevent a packet received on a SAP within the group from being propagated to other members of the group.

SHGs are defined when you create or modify a VPLS site. You can create multiple SHGs for a VPLS site. SHGs can support a mix of spoke SDPs and SAPs. When you create SAPs or spoke SDPs they can be associated with an SHG.

Users can:

- configure, modify, or delete SHGs on a VPLS site
- associate SAPs or spoke SDPs with SHGs

Residential split horizon groups

RSHGs are SHGs with the Residential parameter enabled. SAPs that are associated with RSHGs are called lightweight SAPs. RSHGs use dual-pass queue optimization and do not support downstream broadcast or multicast traffic.

Users can:

- configure, modify, or delete RSHGs on a VPLS site
- associate SAPs or spoke SDPs with RSHGs

Note — If a SAP or spoke SDP is associated with an RSHG, then the following apply:

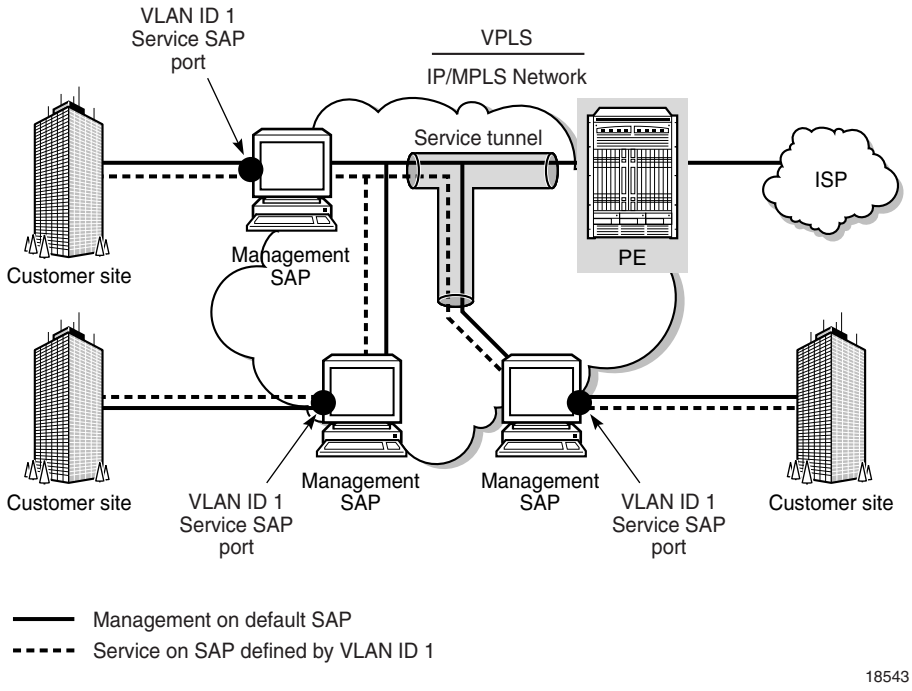
- MAC pinning is enabled by default and cannot be disabled for the interface
- IGMP snooping, MLD snooping, and MVR are not configurable for the interface

Default SAPs

The 5620 SAM allows you to create a default SAP that you can use in an L2-based service to perform management tasks or to deliver a specific class of end-user service. One default SAP can be defined on any dot1q encapsulated Ethernet port. You can create a default SAP by specifying an outer encapsulation value of 4095 or *. If OSSI is used, the outer encapsulation value is always 4095.

Figure 68-10 shows a default SAP used as a dedicated management port.

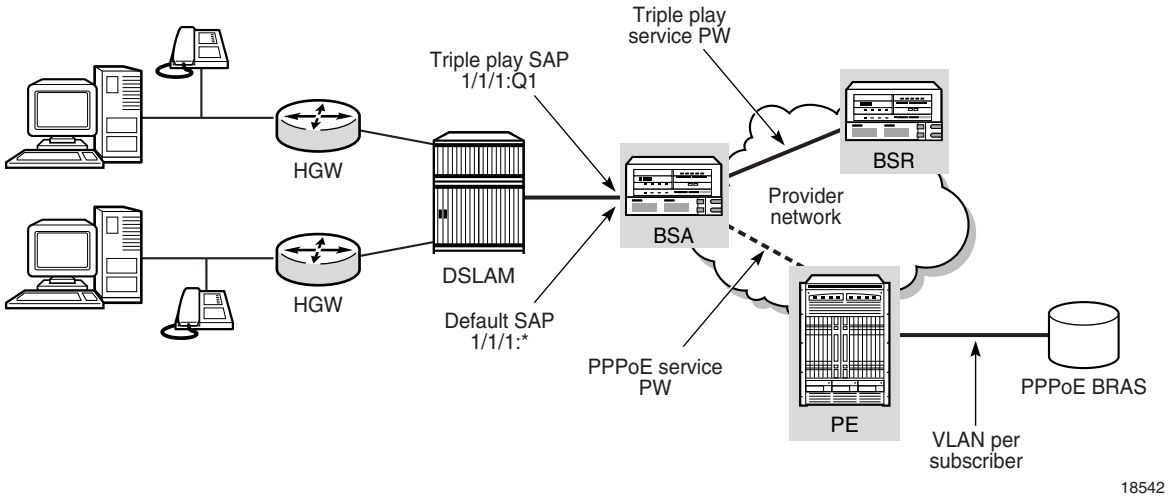
Figure 68-10 Default SAP as a dedicated management port



The dotted line shows that a business customer uses an entire port to access an L2 service using a VLAN tag ID 1, which is transparent to the network service provider. The service provider has assigned a default SAP for management of the customer network, as shown by the solid line. The customer uses one SAP for service delivery, and the service provider uses the default SAP to manage the customer network.

Default SAPs can also be used to differentiate one class of service from another on a single port. In Figure 68-11 the service provider can deliver aggregated high-speed Internet services on a single default SAP for multiple hosts while applying tags that assign one VLAN per host. At the same time, each of the remaining SAPs on the same port can be deployed for higher-level services, such as triple play delivery, in which multiple or individual hosts are assigned to a single SAP. Using such differentiated SAPs is efficient and significantly increases network scalability, because of the reduced number of SAPs allocated to various customers.

Figure 68-11 Default SAP to differentiate subscriber services



Layer 2 protocol tunneling termination

L2PT allows service providers to preserve the VLAN and Layer 2 protocol configurations of individual customers without impacting the traffic of other customers across the core network. L2PT termination allows Layer 2 PDUs to be transparently tunneled across the core network, avoiding interaction between the network provider and customer protocols.

Transparent L2PT is performed on the ingress side of every SAP or spoke SDP of the PE routers configured with L2PT termination. L2PT tunnels PDUs by overwriting the customer PDU of the destination MAC address in an Ethernet packet the multicast MAC address 01-00-0c-cd-cd-d0. The Ethernet packet is then transparently tunneled over the core network to a peer PE router. The peer PE router at the egress side of the tunnel restores the MAC address and the L2 protocol so that packets are forwarded to all ports in the same VLAN.

L2PT termination can only be enabled if STP is disabled on the VPLS.

BPDU translation

VPLS networks typically interconnect customer sites that use different access technologies, such as Ethernet and bridge-encapsulated ATM PVCs. Because of this, BPDU translation may be necessary to provide end-to-end interconnectivity.

If BPDU translation is enabled on a SAP or spoke SDP, the device intercepts all BPDUs and performs the required translation.

BPDU translation can be enabled only on a SAP or spoke SDP binding if STP is disabled on the VPLS.

DoS protection

To protect a VPLS from a high incoming packet rate that characterizes a DoS attack, you can use the 5620 SAM to create DoS protection policies for the VPLS L2 access interfaces. A DoS protection policy limits the number of control-plane packets that an interface receives each second, and optionally logs a violation notification if a policy limit is exceeded. You can use the NE System Security form to view the violations for a specific NE.

You can configure a DoS protection policy to control the following on a VPLS L2 access interface:

- the control-plane packet arrival rate per subscriber host on the interface
- the overall control-plane packet arrival rate for the interface
- whether an NE sends a notification trap if a policy limit is exceeded

Each VPLS L2 access interface on an NE that supports DoS protection is automatically assigned a default DoS protection policy. The default policy limits only the overall packet arrival rate for the interface, and cannot be deleted or modified. See "To configure an NE DoS protection policy" in the *5620 SAM System Administrator Guide* for information about creating a DoS protection policy.

DDoS protection

You can configure a DDoS protection policy on a VPLS L2 access interface, I-VPLS I-L2 access interface, MVPLS L2 access interface, or I-MVPLS I-L2 access interface. See "To configure an NE DDoS protection policy" in the *5620 SAM System Administrator Guide* for information about configuring a DDoS protection policy.

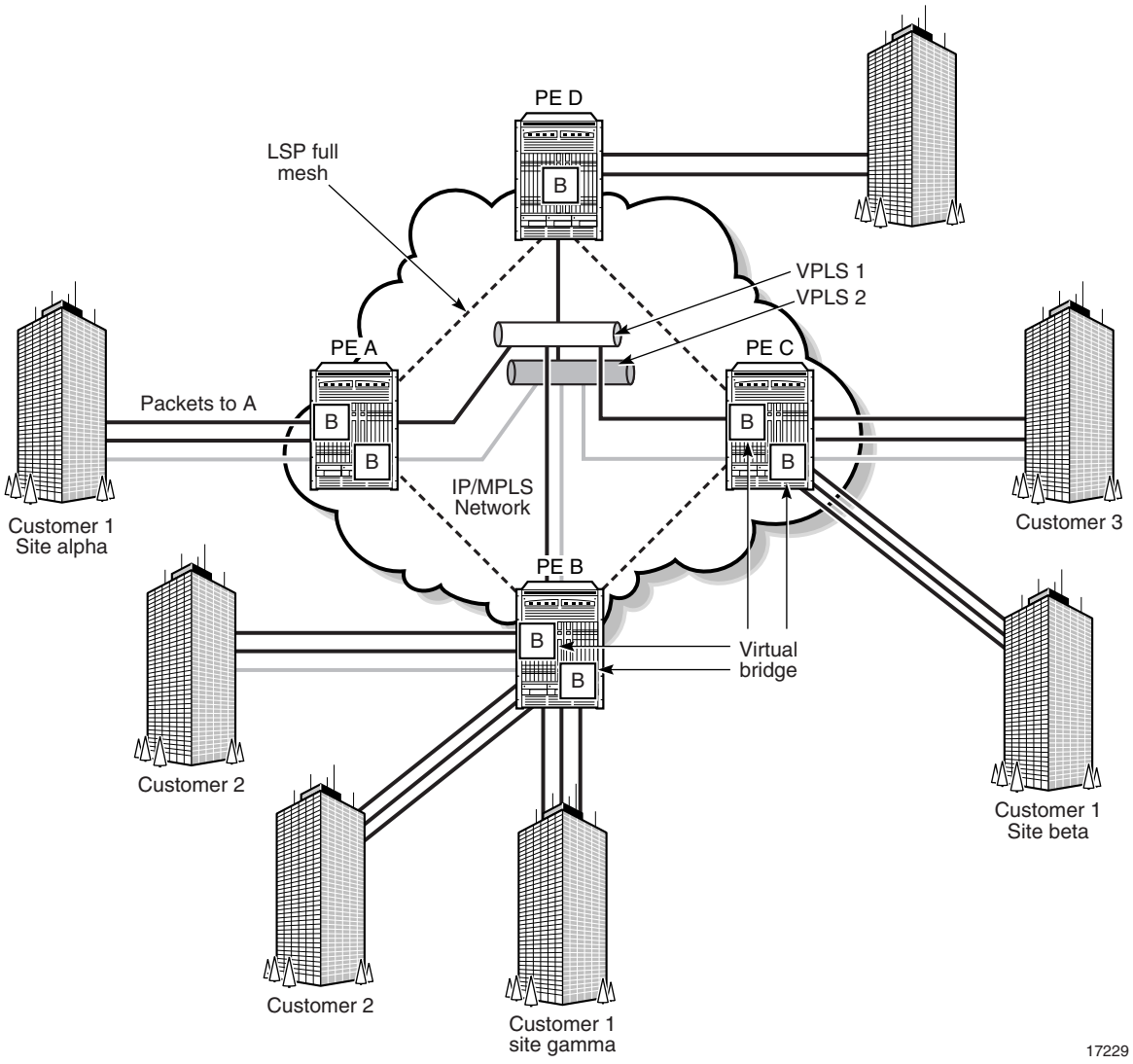
Copying and moving SAPs between ports

You can copy and move SAPs between ports. See "Moving and copying SAPs between ports" in chapter 16 for more information.

68.2 Sample VPLS configuration

Figure 68-12 shows a sample VPLS configuration.

Figure 68-12 Sample VPLS



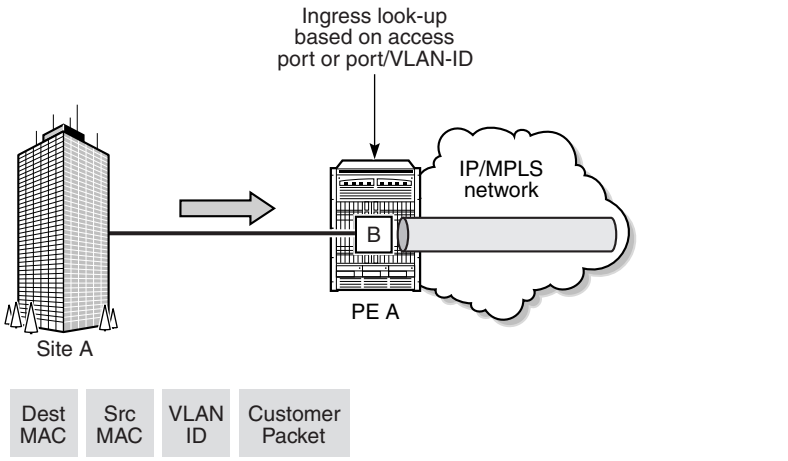
VPLS 1 is a distributed service, which consists of customer 1 connected to PE A, PE B, and PE C, at sites alpha, gamma, and beta, respectively. All three customer sites belong to VPLS 1.

In the following example, Customer 1 wants to send data from site alpha to site beta.

Customer 1 packets arriving at PE A are associated to the appropriate VPLS 1 for that customer, based on the combination of the access port and the dot1q (VLAN ID) in the packet. PE A learns the source MAC address in the packet and creates an entry in the FIB table that associates the MAC address to the access port on which it was received.

PE A is sending the packets to PE C. The destination MAC address in the packet is looked up in the FIB table of PE A for the VPLS instance, as shown in Figure 68-13.

Figure 68-13 Packet forwarding by ingress router PE A



The destination MAC address in the FIB table has one of two values:

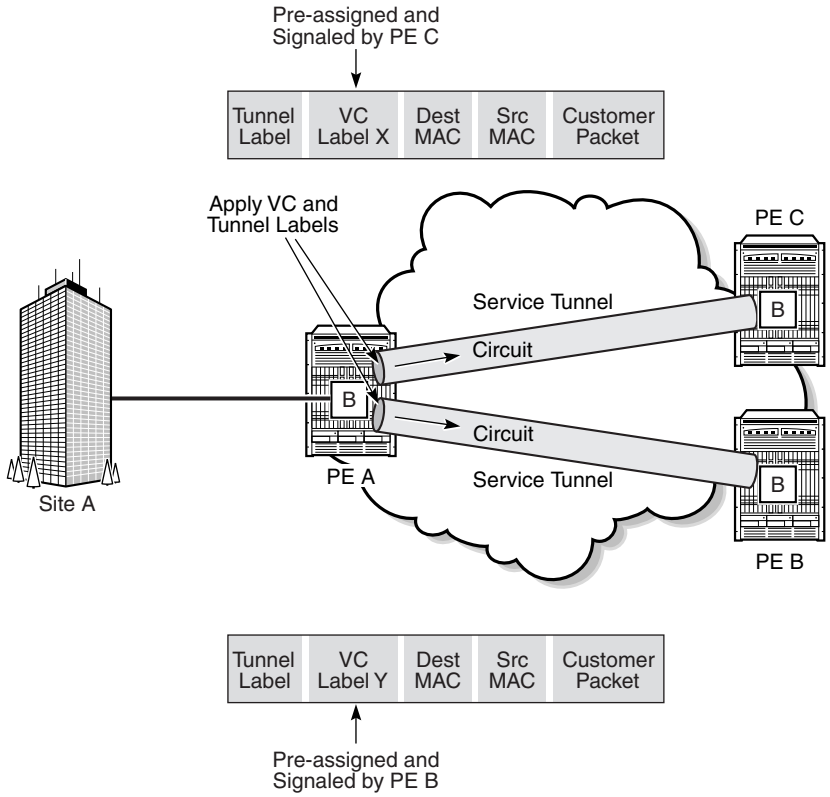
- known
- unknown

If the destination MAC address is known by PE A, an existing entry in the FIB table identifies the far-end PE C and the service VC label (VLAN ID) used to send the packets from PE A to PE C. PE A chooses a transport LSP to send the packets to PE C. The packets from the customer 1 site alpha to site beta are sent on the LSP after the VC label is removed and the transport label is added to the packet, as shown in Figure 68-13.

If the destination MAC address is not known by PE A, PE A floods packets to both PE B and PE C, which are both part of VPLS 1. PE A uses the VC labels (VLAN IDs) that PE B and PE C previously signaled for this VPLS 1.

As shown in Figure 68-14, the packets from PE A are transported across the core IP/MPLS network.

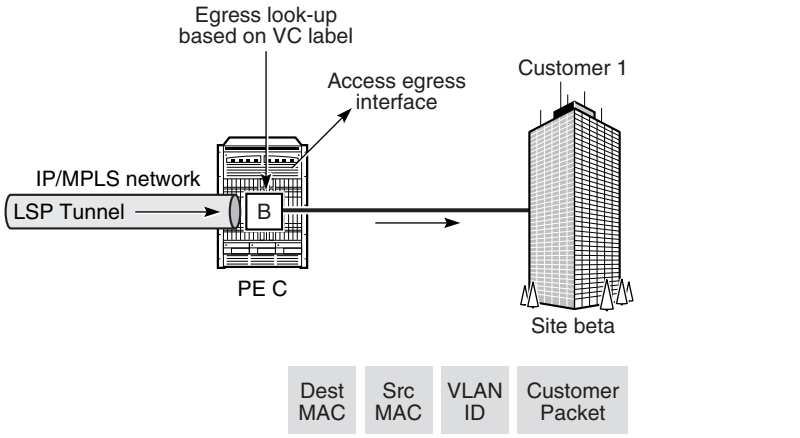
Figure 68-14 Packet forwarding from PE A across the core IP/MPLS network



The core routers are LSRs that switch the packets towards their destination based on the tunnel label, also called a transport label. The core routers are not aware that the packets belong to a VPLS.

When the packets from PE A arrive at PE C, PE C removes the tunnel label to reveal the VC label that associates the packets with VPLS 1, as shown in Figure 68-15.

Figure 68-15 Packet forwarding by egress router PE C



PE C learns the source MAC address of PE A and creates an entry in its FIB table that associates the MAC address and the VC label with PE A. The destination MAC address is looked up in the FIB table. It has one of two values:

- known
- unknown

If the destination MAC address is known by PE C, an existing entry in the FIB table identifies the local access (egress SAP) port used by VPLS 1 site beta and the service VC label (VLAN ID) that needs to be added to send the packets from PE C to customer 1.

If the destination MAC address is not known by PE C, PE C floods packets to all local access ports that belong to VPLS 1.

Assuming the core IP/MPLS network has already been configured, the following high-level tasks are required to configure this sample VPLS.

Table 68-1 Sample VPLS configuration

Task	Description
1. Configure policies as required	Policies must be configured before service creation. The following key policies can be applied to resources that are part of a VPLS: • Access ingress and access egress policies. Choose Policies→QoS→SROS QoS→Access Ingress or Access Egress, then the name of the form you want to configure, to open the access ingress and egress interface policy forms. • Scheduler policy. Choose Policies→QoS→SROS QoS→Scheduler, then the name of the form you want to configure, to open the scheduler policy forms. • ACL MAC filter policies. These policies specify access control lists based on MAC addresses. You can specify MAC learning for access ports or tunnels. Choose Policies→Filter→ACL MAC Filter to open the ACL filter policy form. • Accounting policy. Choose Tools→Statistics→Accounting Policies to open the accounting policy form. • ANCP policy. Choose Policies→Residential Subscriber to open the Manage Subscriber Policies form. • DoS protection policy. Choose Administration→Security→NE DoS Protection to open the NE DoS protection form. • DDoS protection policy. Choose Administration→Security→NE DDoS Protection to open the NE DDoS protection form.
2. Configure ports as access ports for use in the service	Choose a port from the navigation tree, right click on the port, and choose Properties. Specify the port as an access port and specify an encapsulation type, if required.
3. Configure service tunnels, as required.	Service tunnels, or SDPs, are automatically created if there are no tunnels between the source and destination devices. You must choose GRE or LDP as the transport type for the 5620 SAM to automatically create service tunnels. To manually create service tunnels, choose Manage→Service Tunnels. Service tunnels carry service traffic between edge-managed routers. Services are associated with service tunnels by SDP bindings during service configuration. During service creation, you can also configure the 5620 SAM to automatically create SDP bindings to associate service tunnels with a service. In this case, you do not have to create service tunnels before you create the service.
4. Create and configure Customer 1.	Choose Manage→Service→Customers to open the customer manager form and create the customer.

(1 of 3)

Task	Description

5. Create and configure VPLS 1.	• Specify Customer 1 as the customer for the VPLS.
	• Configure MVR for the VPLS, if required.
	• Configure a GSMP Group and a GSMP group neighbor for the VPLS, if required.
	• Configure L2 management interfaces, if required.
	• Specify PE A, PE B, and PE C as the sites for the VPLS.
	• Specify VPLS STP parameters, if required.
	• Specify VPLS FIB parameters, if required.
	• Specify VPLS MAC move parameters, if required.
	• Specify VPLS MAC flush parameters, if required.
	• Enable VPLS PIM snooping, if required.
	• Specify VPLS IGMP snooping parameters, if required.
	• Specify VPLS MLD snooping parameters, if required.
	• Create an SHG for the VPLS, if required.
	• Configure and specify access interfaces on the PE A and PE C sites as the access interfaces for the VPLS to site alpha and site beta. You do the following when you configure interfaces:
	  • Specify the ports for the access interfaces and configure the access interfaces. Ports must be configured as access ports.
	  • Specify the EMG to which the L2 access interface belongs.
	  • Assign ingress and egress QoS policies as required.
	  • Assign an aggregation scheduler for traffic rate limiting across the card or port, if required. Otherwise, assign ingress and egress scheduler policies.
	  • Assign ACL filter policies as required.
	  • Assign an accounting policy, if required.
	  • Specify a ToD suite, if required.
	  • Configure STP and FIB forwarding control.
	  • Configure subscriber management parameters, if required.
	  • Assign a DoS protection policy, if required.
	  • Configure VPLS PIM snooping, if required.
	  • Configure IGMP snooping for the interface, if required.
	  • Configure MLD snooping for the interface, if required.
	  • Configure DHCP for the interface, if required.
	  • Configure ARP host configuration, if required.
	  • Configure MVR for the interface, if required.
	  • Configure anti-spoofing for the interface, if required.
	  • Associate MEPs with SDP spoke bindings or SAPs, if required.
	  • Associate virtual MEPs with services, if required.
	  • Configure ANCP, if required.
	  • Configure ATM functionality, if required.
	• Create and configure service tunnels in both directions.
	• If the VPLS is a distributed VPLS, configure mesh SDP bindings to connect the VPLS sites. You can also configure the 5620 SAM to automatically create SDP bindings.

6. Create, update, or configure additional sites or L2 access interfaces for the VPLS.	• Repeat the above steps as required. • Create an MSAP policy, if required. See Procedure 54-5 for more information about creating an MSAP policy. • Configure the SAP Sub Type to be created. If your SAP is to support a shared SAP model, configure a Regular SAP; that is choose Regular as the SAP Sub Type. If you need to use an MSAP to support the one subscriber per SAP model, choose Capture as the SAP Sub Type and then configure the Capture L2 Interface parameters, which control the DHCP, PPPoE, or ARP triggered creation of MSAPs. See Managed SAP (MSAP) in section 65.1 for more information about creating a Capture SAP and MSAP.
7. For an HVPLS, use spoke SDP bindings to connect VPLS sites to other sites in the same VPLS, to sites in a different VPLS, or to VLL service sites.	An HVPLS consists of VPLS sites connected to other VPLS sites in the same or different VPLS, or to VLLs, using spoke SDP bindings. You perform the following when you configure an HVPLS. • Create one or more VPLS and VLL services, as required. See chapter 67 for information about creating a VLL service. See Procedure 68-1 in this chapter for information about creating a VPLS. • Create spoke SDP bindings between the service sites, one in each direction. Specify existing service tunnels and a VC ID for the spoke SDP bindings, as required.

(2 of 3)

Task	Description
8. Create a single MVPLS.	Create an MVPLS to run RSTP and to protect redundant spoke SDPs or SAPs in the associated VPLS.
9. Create a composite MVPLS to manage traffic blocking for multiple VPLS.	An MVPLS composite service manages traffic for multiple VPLS with redundant spoke SDPs or SAPs. You perform the following when you configure an MVPLS composite service. • Create a composite service and add the individual MVPLS. • Create spoke SDP connectors between the MVPLS.

(3 of 3)

68.3 Workflow to create a VPLS

The following workflow lists the high-level steps required to create a VPLS. As a prerequisite for creating a VPLS, this workflow assumes the following:

- a group or customer with the required user access privileges has been set up.
- the IP or IP/MPLS core network exists.
- any required service tunnels are created including the static or dynamic LSP required to create the service tunnel. See Procedure 27-1.
- the access ports for the service are created. See chapter 16 for more information.
- any required pre-defined routing, QoS, scheduling, filter, accounting, and time of day suite policies are created. See chapter 42 for more information. You do not have to create pre-defined policies if policies are created on a per-service basis.
- any required MP-BGP for PE-to-PE routing is configured. See chapter 23 for more information about protocol configuration.

1 Create and configure a VPLS. See Procedure 68-1.

i Define the service type as VPLS.

ii Ensure the LSP network is configured when the transport mechanism is MPLS.

iii Configure HVPLS spoke redundancy, if required.

2 Specify the sites for the service. See Procedure 68-7.

i Specify the STP parameters, if required. See Procedure 68-8.

ii Create MSTP instances and associate VLANs, if required. See Procedure 68-8.

iii Specify protected MAC addresses, if required. See Procedure 68-8.

iv Configure subscriber management on the site, if required. See Procedure 68-9.

v Configure a default gateway for the site, if required. See Procedure 68-10.

vi Configure ingress multicast forwarding for the site, if required. See Procedure 68-11.

vii Configure a provider tunnel for the site, if required. See Procedure 68-12.

viii Specify the service tunnel required bandwidth for the site, if required. See Procedure 68-13.

ix Configure IGMP snooping on the site, if required. See Procedure 68-14.

x Configure the split horizon group parameters, if required. See Procedure 68-16.

xi Configure MVR, if required. See Procedure 68-17.

xii Configure GSMP group and GSMP group neighbor parameters, if required. See Procedure 68-18.

xiii Create L2 management interfaces on the site, if required. See Procedure 68-19.

xiv Configure MLD snooping on the site, if required. See Procedure 68-20.

xv Associate a virtual MEP to the site, if required. See Procedure 68-21.

xvi Configure MVR for MLD on the site, if required. See Procedure 68-22.

xvii Configure IGMP host tracking on the site, if required. See Procedure 68-23.

3 Create L2 access interfaces for the VPLS sites, as required. See Procedure 68-24.

i Specify aggregation on a service basis, or across a card or port.

ii Configure MSAP policies, if required. Create an MSAP Policy to control how the parameters are applied to an MSAP when it is automatically created. See Procedure 54-5 for more information.

iii Configure the SAP Sub Type as Regular or Capture, as required. Regular is the default value used for the creation of a SAP and Capture is the value used to enable the automatic creation of an MSAP. That is, you create a Capture SAP to enable the creation of an MSAP. See Procedure 65-28 for more information about creating a Capture SAP.

iv Assign QoS, scheduling, accounting, and filter policies. See Procedure 68-24.

v Specify MAC ACL filters, if required. See Procedure 68-24.

vi Assign a time of day suite, if required. See Procedure 68-24.

vii Configure queue override parameters, if required. See Procedure 68-24.

viii Configure the BPDU Termination, STP, and FIB parameters. See Procedure 68-27.

ix Assign a DoS protection policy or DDoS protection policy, if required. See Procedure 68-28.

x Configure subscriber management, if required. See Procedure 68-29.

xi Configure ethernet tunnels, if required. See Procedure 68-30.

xii Configure a redundant VLAN range, if required. See Procedure 68-31.

xiii Configure IGMP snooping parameters, if required. See Procedure 68-32.

xiv Configure ARP hosts, if required. See Procedure 68-33.

xv Configure DHCP relay parameters, if required. See Procedure 68-34.

xvi Configure MVR, if required. See Procedure 68-35.

xvii Configure anti-spoofing parameters, if required. See Procedure 68-36.

xviii Associate a MEP to the interface, if required. See Procedure 68-37.

xix Assign an ANCP policy, if required. See Procedure 68-38.

xx Configure PIM snooping parameters, if required. See Procedure 68-39.

xxi Configure MLD snooping parameters, if required. See Procedure 68-40.

xxii Configure MVR for MLD, if required. See Procedure 68-41.

xxiii Configure custom object attributes for AA reporting to the 5670 RAM, if required. See Procedure 68-42.

4 Create endpoints on the site for redundant configuration, if required. See Procedure 68-15.

5 Create a spoke SDP binding under any endpoints you created on the site, if required. See Procedure 68-44.

6 Create a mesh SDP binding for the VPLS site, if required. See Procedure 68-43.

7 Create a spoke SDP binding for the VPLS site, if required. See Procedure 68-44.

8 Configure the following on the SDP binding, as required.

i Assign a DoS protection policy, if required. See Procedure 68-46.

ii Configure the MFIB, STP, and FIB parameters. See Procedure 68-47.

iii Configure DHCP for the SDB binding, if required. See Procedure 68-48.

iv Configure IGMP snooping parameters, if required. See Procedure 68-49.

v Associate a MEP to the interface, if required. See Procedure 68-50.

vi Configure MLD snooping parameters, if required. See Procedure 68-51.

vii Configure PIM snooping parameters, if required. See Procedure 68-52.

viii Configure custom object attributes for AA reporting to the 5670 RAM, if required. See Procedure 68-53.

9 Create and enable a video interface for the VPLS, if required. See Procedure 30-3.

10 Configure a site for BGP AD or BGP VPLS, as required. See Procedure 68-54.

i Create a routing policy to define the required community members. See Procedure 22-15.

ii Enable BGP on the routing instance of each NE in the VPLS or BGP VPLS. See Procedure 23-1.

iii Configure global-level BGP on each NE in the VPLS or BGP VPLS. See Procedure 23-2.

iv Create a PW template policy. See chapter 73 for information about PW template policies.

v Distribute the PW template policy to each NE that is or will be a component of the VPLS or BGP VPLS.

vi Configure a site for BGP VPLS Multi-homing, is required. See Procedure 68-55.

vii Create SDPs for the BGP VPLS Multi-homing site(s), if manually-provisioned service tunnels are required. See Procedure 27-1.

viii Re-evaluate the PW template policies associated with a BGP AD or BGP VPLS site when a policy is modified, if required. See Procedure 68-56 and Procedure 73-3.

11 Perform one or more of the following.

a Create an HVPLS. See Procedure 68-58.

b Create an MVPLS. See Procedure 68-59.

c Create a B-site for VPLS or MVPLS. See Procedure 68-60.

d Create an I-VPLS. See Procedure 68-65.

e To create a VPLS or MVPLS B-L2 access interface. See Procedure 68-66.

f Create a VPLS I-L2 access interface. See Procedure 68-70.

g Configure a GNE site on a VPLS service. See Procedure 68-71.

h Force a switchover to a redundant spoke SDP binding. See Procedure 68-72.

i Run an OAM validation test for a VPLS. See Procedure 68-73.

12 As required, modify the FIB entries associated with a VPLS:

a Add or modify FIB entries. See Procedure 68-74.

b List FIB entries. See Procedure 68-75.

13 As required, view VPLS information:

a View the service topology map associated with a VPLS. See Procedure 68-76.

b View the VPLS operational status. See Procedure 68-77.

c View IGMP snooping queriers. See Procedure 68-78.

d View MLD snooping queriers. See Procedure 68-79.

14 As required, modify a VPLS:

a Using the Manage Services form. See Procedure 68-80.

b Using the topology view. See Procedure 68-81.

15 As required, delete a VPLS. See Procedure 68-82.

68.4 VPLS management procedures

Use the following procedures to perform VPLS creation and management tasks.

Procedure 68-1 To create a VPLS

1 Choose Create→Service→VPLS from the 5620 SAM main menu. The VPLS Service (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the VPLS. The Select Customer - VPLS Service form opens.

3 Choose a customer for the VPLS and click on the OK button. The Select Customer - VPLS Service form closes, and the VPLS Service (Create) form displays the customer information.

4 Configure the parameters:

- Service ID
- Auto-Assign ID
- SVC Mgr Service ID
- Service Name
- Description
- Service Tier
- Service Priority
- Administrative State
- Default Mesh VC ID
- Inherit Service ID Value
- Automatic Mesh SDP Binding Creation

The Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.

The SVC Mgr Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.

The Default Mesh VC ID parameter is configurable when the Inherit Service ID Value parameter is disabled.

5 Configure the OLC state:

i Click on the Apply button.

ii Configure the parameters:

- Current OLC State
- Revert OLC State

6 If you enabled the Automatic Mesh SDP Binding Creation parameter in step 4, perform the following steps. Otherwise, go to step 7.

i Click on the Select button beside the Profile Name parameter. The Select Tunnel Selection Profile - VPLS Service - Subscriber form opens.

ii Choose a tunnel selection profile from the list and click on the OK button. The Select Tunnel Selection Profile - VPLS Service - Subscriber form closes and the VPLS Service (Create) form refreshes with the tunnel selection profile information.

iii Configure the Transport Type parameter. The Transport Type parameter is configurable only when the Profile Name parameter is not configured.

7 Click on the OK button. The VPLS Service (Create) form closes.

Procedure 68-2 To configure a VPLS for AA reporting to the 5670 RAM

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services is displayed.

3 Choose a VPLS in the list and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 Click on the Application Assurance tab. The 5670 RAM Parameters tab is displayed.

5 Configure the parameters:

- Enable Application Performance Reporting
- Report Customer Name
- Number of IP Detail Addresses

6 To configure one or more custom DCP groups, see the custom DCP group configuration procedure in chapter 76.

7 To specify an application or application group for IP detail reporting, click on the IP Detail Application or IP Detail Application Group tab, as required. The IP Detail Application or IP Detail Application Group (Create) form opens.

Otherwise, go to step 13.

8 Configure the parameters:

- ID
- Auto-Assign ID

9 Click on the Select button and choose an application or application group from the Select Application or Select Application Group form.

10 Click on the OK button. The IP Detail Application or IP Detail Application Group (Create) form closes, and a dialog box appears.

11 Click on the OK button. The application or application group is listed on the VPLS Service (Create) form.

12 To specify another application or application group for IP detail reporting, repeat steps 7 to 11.



Note — You can specify up to 10 applications and up to 10 application groups.

13 Close the VPLS Service (Edit) form.

14 Close the Manage Services form.

Procedure 68-3 To assign a multicast package policy to a VPLS

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 Click on the Multicast tab.

5 Click on the MVR tab.

6 Click on the Select button to choose a multicast package policy. The Select Multicast Package Policy - VPLS Service - Subscriber form opens.

7 Choose a multicast package policy and click on the OK button. The Select Multicast Package Policy - VPLS Service - Subscriber form closes, and the VPLS Service (Create) form refreshes with the multicast package policy name.

After the multicast package policy is applied to the VPLS, the policy is distributed as the routing policy to all MVR-capable VPLS sites. If you apply another package policy to the site, the new policy is distributed to the site. The previously distributed policy remains on the site.

8 Click on the OK button. The VPLS Service (Edit) form closes.

9 Close the Manage Services form.

Procedure 68-4 To configure bandwidth management for a VPLS



Note — In order to configure required bandwidth, you must enable multi-segment tunnel selection and service bandwidth management at the system level.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 Click on the Bandwidth button.

5 Click on the Required Bandwidth tab to configure service tunnel required bandwidth for the service, if required.

6 Configure the Bandwidth Method parameter.

7 If you set the Bandwidth Method parameter to Input Manually or Calculate From SAPs, configure LSP Path Booking parameter.

8 If you the Bandwidth Method parameter to Input Manually, enter a required bandwidth value for each CoS (see CoS 0 Bandwidth - CoS 7 Bandwidth).

9 Click on the Bandwidth Reserved Tunnel tab to reserve PBB tunnel bandwidths, if required.

10 For each CoS, enter a value for the CoS Reserved Bandwidth (Mbps) to specify how much bandwidth this tunnel will reserve in the network.

11 Click on the Reserve Bandwidth button. This action checks to ensure that all the active links in the B-VPLS have enough bandwidth to admit the tunnel into the network and book the bandwidth. The tunnel status will be updated appropriately, based on the outcome of the action. Once the bandwidth is reserved, the BW Utilization tab on the applicable Physical Link properties form will also show this tunnel and the bandwidth information. See Procedure 6-37 for more information.



Note 1 — The reserved bandwidth of the tunnel can be changed at any time after the service creation. However, if a change to the reserved bandwidth causes the used bandwidth to be greater than the requested change, or if there is insufficient bandwidth in the network to facilitate this change, then it will be denied and an appropriate message is displayed.

Note 2 — Once bandwidth is reserved on the tunnel, any changes to the topology of the B-VPLS (for example, uplinks added, STP state changes, and so forth) will be updated automatically with the correct bandwidth information on the underlying physical links. If there is insufficient bandwidth available when the changes happen, the bandwidth will still be booked on the physical links and the appropriate alarms will be raised.

Note 3 — To unreserve bandwidth of the tunnel after the service creation, you can set all of the configured Cos Reserved Bandwidth parameters back to 0. However, this can only be done when there are no longer any i-services riding on this PBB Tunnel.

Note 4 — After the service has been created, the Tunnel Usage tab shows all the i-services currently using this tunnel and the specific bandwidth usage per service.

12 Click on the OK button. The VPLS Service (Edit) form closes.

13 Close the Manage Services form.

Procedure 68-5 To configure the VPLS for BGP auto-discovery

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 Click on the BGP AD tab.

5 Set the BGP AD Administrative Status parameter to Up. The BGP AD Service Identification group appears.

6 Configure the VPLS ID parameter. This parameter must be a unique network-wide ID.

7 Click on the OK button. The VPLS Service (Edit) form closes.

8 Close the Manage Services form.

Procedure 68-6 To add protected MAC addresses to a VPLS



Note — Protected MAC addresses that you add at the VPLS site level are automatically added at the service level. See step 12 of Procedure 68-7 for more information about adding protected MAC addresses at the site level.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 Click on the Forwarding Control tab.

5 Click on the MAC Protection tab.

6 Click on the Create button. The MAC Protection (Create) form opens.

7 Configure the Protected Mac Address parameter.

8 Click on the OK button. The MAC Protection (Create) form closes and the protected MAC address is listed on the VPLS Service (Create) form.

9 Click on the OK button. The VPLS Service (Edit) form closes.

10 Close the Manage Services form.

Procedure 68-7 To configure a VPLS site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 Perform one of the following.

a Create a VPLS site by performing the following steps:

i On the navigation tree, right-click on Sites and choose Create VPLS Site. The Select Network Elements - VPLS Service - Subscriber form opens with a list of available sites.

ii Select a site and click on the OK button. The VPLS Site (Create) form opens with the General tab displayed.



Note — The options to create either a B-Site or an I-Site are used when you are configuring a VPLS that utilizes Provider Backbone Bridging. See "Provider Backbone Bridging in VPLS" in section 68.1 for more information.

b Configure an existing VPLS site by performing the following steps:

i Expand the Sites icon in the service navigation tree.

ii Right-click on a site icon and choose Properties from the contextual menu. The VPLS Site (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Name
- Description
- MTU
- Administrative State
- Monitor Access Interface Operational State

6 Configure the NE-specific parameters, as listed in Table 68-2.

Table 68-2 NE-specific parameters

NE	Parameters	Dependencies
7750 SR, 7450 ESS, 7710 SR, 7950 XRS	• Default Mesh VC ID • GSMP Administrative State • PIM Snooping Enabled • Per Service Hashing for LAG Enabled • Enable IP Interface Binding • Tunnel Fault Notification	The Enable IP Interface Binding parameter is configurable only on the 7950 XRS, the 7450 ESS in mixed mode and the 7750 SR, Release 8.0 R5 and later. Tunnel Fault Notification is configurable on sites where the device has ports configured in access or hybrid mode with QinQ encapsulation. If you are configuring a tunnel facility MEP, Tunnel Fault Notification must be set to Accept, in order to accept the fault propagation from the tunnel facility MEP.

(1 of 2)

NE	Parameters	Dependencies
7210 SAS-D, 7210 SAS-E, 7210 SAS-M, 7210 SAS-T, 7210 SAS-X	• Customer VID • SAP Type	The Customer VID parameter is configurable only when the SAP Type parameter is set to dotq1-preserve.
7210 SAS-M, 7210 SAS-X	• Enable MTU Check	No dependencies.
7705 SAR	• PPPoE Circuit ID	No dependencies.

(2 of 2)

7 Click on the OK button. The VPLS Site (Create) form closes, and a dialog box appears.

8 Click on the OK button.

9 Repeat steps 4 to 8 to create an additional site for the VPLS, as required.

10 To configure MFIB, STP, FIB, and MAC learning protection parameters for the VPLS site, perform Procedure 68-8.

11 To configure SHCV on the VPLS site, perform Procedure 68-9.

12 To configure a default gateway on the VPLS site, perform Procedure 68-10.

13 To configure ingress multicast forwarding on the VPLS site, perform Procedure 68-11.

14 To configure a provider tunnel on the VPLS site, perform Procedure 68-12.

15 To configure service tunnel required bandwidth on the VPLS site, perform Procedure 68-13.

16 To configure IGMP snooping on the VPLS site, perform Procedure 68-14.

17 To create an endpoint for redundancy on the VPLS site, perform Procedure 68-15.

18 To configure SHG on the VPLS site, perform Procedure 68-16.

19 To configure MVR for the VPLS site, perform Procedure 68-17.

20 To configure a GSMP group on the VPLS site, perform Procedure 68-18.

21 To configure a L2 management interfaces on the VPLS site, perform Procedure 68-19.

22 To configure MLD snooping on the VPLS site, perform Procedure 68-20.

23 To configure MVR for MLD on the VPLS site, perform Procedure 68-22.

24 To configure IGMP host tracking on the VPLS site, perform Procedure 68-23.

25 To create an access interface for the site, perform Procedure 68-24.

26 To create a mesh SDP binding for the site, perform Procedure 68-43.



Note 1 — The maximum combined number of mesh and spoke SDP bindings that you can configure on a service site depends on the NE type and release on which the site is configured. A deployment error occurs when you attempt to create an SDP binding if this limit is reached on the NE.

Note 2 — The maximum number of VPLS sites that can be automatically connected using mesh SDP bindings is 100. You can perform automatic creation of a full mesh in a VPLS in one or more passes, as required.

Alcatel-Lucent recommends that you perform automatic mesh SDP binding creation on only 50 sites at one time. Performing automatic mesh SDP binding creation on 100 sites at one time may result in a substantial delay in building the network.

27 To create a redundant spoke SDP binding under an endpoint, perform Procedure 68-44.

28 To create a spoke SDP binding for the site, perform Procedure 68-44.



Note 1 — The maximum combined number of mesh and spoke SDP bindings that you can configure on a service site depends on the NE type and release on which the site is configured. A deployment error occurs when you attempt to create an SDP binding if this limit is reached on the NE.

Note 2 — You cannot create a spoke SDP binding on an MVPLS site that runs MSTP, or enable MSTP on a site that has a spoke SDP binding.

Note 3 — You cannot enable MSTP on a SAP that has a non-zero encapsulation value.

29 To add a Video interface for the site, perform Procedure 30-3.

30 To configure the site for BGP Auto-Discovery, BGP VPLS, or as part of a BGP VPLS Multi-homing configuration, you must first complete the creation of the site and then perform either Procedure 68-54 or Procedure 68-55, as applicable.



Note — You can see a list of all current BGP VPLS Multi-homing sites in a VPLS multi-homing service on the BGP Multi-homing Sites tab.

Procedure 68-8 To configure MFIB, STP, FIB, and MAC learning protection for a VPLS site

Perform the following procedure to configure MFIB, STP, FIB, and MAC learning protection parameters for a VPLS site, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure MFIB, STP, FIB, and MAC learning protection parameters and click on the Properties button. The VPLS Site (Edit) form opens with the General tab displayed.

5 Click on the Forwarding Control tab. The MFIB tab is displayed. If you are configuring a 7705 SAR, go to step 7.

6 Configure the parameters:

- Table size (entries)
- High Watermark (%)
- Low Watermark (%)

7 Click on the STP tab to configure the following STP parameters:

- Bridge Hello Time (seconds)
- Priority
- STP Mode
- Maximum BPDUs (PDUs/Hello Interval)
- Administrative State

8 Configure the NE-specific STP parameters, as listed in Table 68-3.

Table 68-3 NE-specific parameters

NE	Parameters	Dependencies
7750 SR, 7450 ESS, 7950 XRS, 7210 SAS-D, 7210 SAS-E	• Bridge Forward Delay (seconds) • Bridge Max Age (seconds)	No dependencies.



Note 1 — Alcatel-Lucent STP in a VPLS interoperates with customer STP implementations as a mechanism for loop detection and prevention. The bridge-level parameters balance the STP resiliency and speed of convergence. Modifying the bridge-level parameters must be done within the constraints of the following formulas:

- 2 × (Bridge Forward Delay – 1.0 s) >= Bridge Max Age
- Bridge Max Age >= 2 × (Bridge Hello Time + 1.0 s)

Note 2 — If you are configuring an MVPLS site, set the STP Mode parameter to RSTP or MSTP, depending on the MVPLS type. The MSTP option is available only if you are creating an MVPLS. See Procedure 68-59 for more information about creating an MVPLS.

Note 3 — MSTP is configurable only on the 7450 ESS, 7750 SR, and 7950 XRS.

9 Click on the FIB tab to configure FIB parameters for the VPLS site, if required.

10 Configure the parameters:

- High Watermark (%)
- Low Watermark (%)
- Local Age Time (seconds)
- Remote Age Time (seconds)
- Size (entries)
- Aging Enabled
- Learning Enabled
- Discard Unknown Destinations
- Move Frequency
- Retry Timeout
- Administrative State

11 Configure the NE-specific parameters, as shown in Table 68-4.

Table 68-4 NE-specific parameters

NE	Parameters	Dependencies
7750 SR, 7450 ESS, 7710 SR, 7705 SAR, 7950 XRS	• MAC Flush on fail • Propagate MAC Flush • MAC Subnet Length • Number of Retries • Primary Ports Cumulative Factor • Secondary Ports Cumulative Factor	No dependencies.

(1 of 2)

NE	Parameters	Dependencies
7210 SAS-D, 7210 SAS-E, 7210 SAS-X	No NE-specific parameters.	

(2 of 2)

12 Click on the MAC Protection tab to configure the list of protected MAC addresses.

13 Click on the Create button. The MAC Protection (Create) form opens.

14 Configure the Protected Mac Address parameter.

15 Click on the OK button to close the form and add the MAC address to the list of protected MAC addresses.

16 If you are configuring an MVPLS site that requires MSTP, click on the MSTP tab. Otherwise, go to step 27.



Note — MSTP is configurable only on the 7450 ESS, 7750 SR, and 7950 XRS.

17 Configure the parameters:

- Region Name
- Region Revision
- Bridge Max Hops

18 Click on the MST Instances tab.

19 Click on the Create button. The MST Instance (Create) form opens with the General tab displayed.

20 Configure the parameters:

- Instance Index
- Priority

21 Click on the VLAN Ranges tab. Click on the Create button. The MST Instance Managed VLAN range (Create) form opens.

22 Configure the parameters:

- Min. VLAN Tag
- Max. VLAN Tag

23 Click on the OK button. The MST Instance Managed VLAN Range (Create) form closes and a dialog box appears.

24 Click on the OK button. The MST Instance (Create) form refreshes with the new managed VLAN range.

25 Click on the OK button. The MST Instance (Create) form closes and a dialog box appears.

26 Click on the OK button. The MVPLS Site (Create) form refreshes with the new MST instance.

27 Click on the OK button. A dialog box appears.

28 Click on the Yes button. The VPLS Site (Edit) form closes.

Procedure 68-9 To configure SHCV for a VPLS site

Perform the following procedure to configure SHCV for the site, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure SHCV and click on the Properties button. The VPLS Site (Edit) form opens with the General tab displayed.

5 Click on the Subscriber Management tab. The Host Connectivity tab is displayed.

6 Select the SHCV Enabled parameter to enable SHCV.

7 Configure the parameters:

- SHCV Interval (minutes)
- SHCV Source IP Address
- SHCV Source MAC Address
- SHCV Action
- SHCV Retry Timeout (seconds)
- SHCV Retry Count

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button. The VPLS Site (Edit) form closes.

Procedure 68-10 To configure a default gateway for a VPLS site

Perform the following procedure to configure a default gateway for the site, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the default gateway and click on the Properties button. The VPLS Site (Edit) form opens with the General tab displayed.

5 Click on the Default Gateway tab.

6 Configure the parameters:

- Default Gateway IP Address
- Default Gateway MAC Address

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The VPLS Site (Edit) form closes.

Procedure 68-11 To configure ingress multicast forwarding on a VPLS site

Perform the following procedure to configure ingress multicast forwarding, if required.



Note — An Operational Channels tab appears when you access the VPLS Site form in the Edit mode. It displays data for the operational channels when traffic from a specific multicast source for a specific multicast group passes through the service. You must click on the Search button to refresh the data. See chapter 42 for information about listing the operational channel parameters.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure ingress multicast forwarding and click on the Properties button. The VPLS Site (Edit) form opens with the General tab displayed.

5 Click on the Multicast tab.

6 Click on the Mcast Path Mgmt tab.

7 Click on the Select button to choose a multicast info policy. The Select Ingress Info Policy - VPLS Site form opens.

8 Choose a policy in the list and click on the OK button. The Select Ingress Info Policy - VPLS Site form closes and the policy identifier is displayed on the Site (Create) form.

9 Click on the OK button. A dialog box appears.

10 Click on the Yes button. The VPLS Site (Edit) form closes.

Procedure 68-12 To configure a provider tunnel for a VPLS site

Perform the following procedure to configure a provider tunnel for the site, if required. When you configure an inclusive provider tunnel, multicast and broadcast Ethernet frames are always forwarded over a P2MP LSP, defined as the Inclusive Provider Multicast Service Interface (I-PMSI). When a provider tunnel is not configured, these frames are replicated at the ingress PE and a copy of each frame is forwarded over the P2P PW to each destination PE participating in the VPLS instance. Provider tunnels can be configured on VPLS and B-VPLS sites.



Note — Provider tunnels are supported on the 7750 SR-7, 7750 SR-12, 7750 SR-c4, 7750 SR-c12, 7750 SR-12E, and 7450 ESS NEs in all chassis modes, as well as on the 7540 ESS, provided all network IP interfaces are on IOM3/IMM ports (chassis mode D).

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure a provider tunnel and click on the Properties button. The VPLS Site (Edit) form opens with the General tab displayed.

5 Click on the Provider Tunnel tab.

6 Enable the Enable Provider Tunnel parameter.

7 Configure the parameters:

- Administrative State
- Data Delay Interval (seconds)
- Root And Leaf
- Type
- LSP Template

The LSP Template parameter is only configurable when the Type parameter is set to RSVP.

The Administrative State parameter is configurable only when the LSP Template parameter has been configured.

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button. The VPLS Site (Edit) form closes.

Procedure 68-13 To configure service tunnel required bandwidth for a VPLS site

Perform the following procedure to configure service tunnel required bandwidth for the site, if required.



Note — In order to configure service tunnel required bandwidth, you must enable multi-segment tunnel selection and service bandwidth management at the system level.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure service tunnel required bandwidth and click on the Properties button. The VPLS Site (Edit) form opens with the General tab displayed.

5 Click on the Bandwidth tab.

6 Enable the Override Service Configuration parameter.

7 Configure the NE-specific parameters, as shown in Table 68-5.

Table 68-5 NE-specific parameters

NE	Parameters	Dependencies
7750 SR, 7450 ESS, 7710 SR, 7950 XRS	• Bandwidth Method	If the Bandwidth Method parameter is set to Input Manually, enter a required bandwidth value for each CoS (see CoS 0 Bandwidth - CoS 7 Bandwidth).

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button. The VPLS Site (Edit) form closes.

Procedure 68-14 To configure IGMP snooping on a VPLS site

Perform the following procedure to configure IGMP snooping for the site, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure IGMP snooping and click on the Properties button. The VPLS Site (Edit) form opens with the General tab displayed.

5 Click on the Multicast tab.

6 Click on the IGMP Snooping tab.

7 Configure the parameters:

- Administrative State
- Query Interval (seconds)
- Robust count
- Report source address
- Use query source address
- Query source address

If the Administrative State is down, packets will be forwarded along the P2P PWs, otherwise they will be forwarded along the P2MP LSP instance.

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button. The VPLS Site (Edit) form closes.

Procedure 68-15 To create an endpoint for redundancy (dual homing) on a VPLS site

Perform the following procedure to create an endpoint for redundancy (dual homing) on the site, if required.



Note — You cannot create a VPLS endpoint on a site that has an active or inactive MC ring SAP. See chapter 41 for more information.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to create an endpoint for redundancy and click on the Properties button. The VPLS Site (Edit) form opens with the General tab displayed.

5 Click on the Endpoints tab.

6 Click on the Create button. The VPLS Endpoint (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Name
- Description
- Revert Time (seconds)
- Disable Revert Time (Infinite)
- Suppress Standby Signalling
- Ignore Standby Signalling
- MAC Pinning
- Maximum FIB Entries
- Block On Mesh SDP Failure

8 Configure the NE-specific parameters, as shown in Table 68-6

Table 68-6 NE-specific parameters

NE	Parameters	Dependencies
7750 SR, 7450 ESS, 7710 SR, 7950 XRS	• Endpoint Type • Restrict Protected Source • Restrict Protected Source Action • Auto Learn MAC Protect • EndPoint ID	The EndPoint ID parameter is configurable only if you set the Endpoint Type parameter to Multi Chassis. The Restrict Protected Source Action parameter is configurable only if you enable the Restrict Protected Source parameter.

9 Click on the OK button. A dialog box appears.

10 Click on the OK button. The Endpoint (Create) form closes and the Site (Create) form reappears with the new endpoint displayed in the list.

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The VPLS Site (Edit) form closes.

Procedure 68-16 To configure an SHG on a VPLS site

Perform the following procedure to configure an SHG on the VPLS site, if required.



Note — You must configure an SHG or RSHG if you plan to create a spoke circuit from this VPLS site to a VLL or to another VPLS.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure SHG and click on the Properties button. The VPLS Site (Edit) form opens with the General tab displayed.

5 Click on the Split Horizon Groups tab.

6 Click on the Create button. The Site, New Split Horizon Group (Create) form opens.

7 Configure the parameters:

- Name
- Description

8 Configure the NE-specific parameters, as shown in Table 68-6

Table 68-7 NE-specific parameters

NE	Parameters	Dependencies
7750 SR, 7450 ESS, 7710 SR, 7950 XRS	• Residential • Restrict Protected Source • Restrict Protected Source Action • Restrict Unprotected Destination • Auto Learn MAC Protect	The Restrict Protected Source Action parameter is configurable only if you enable the Restrict Protected Source parameter.

(1 of 2)

NE	Parameters	Dependencies
7705 SAR	• Residential	No dependencies.

(2 of 2)

9 Click on the OK button. The Site, New Split Horizon Group (Create) form closes.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The VPLS Site (Edit) form closes.

Procedure 68-17 To configure MVR for a VPLS site

Perform the following procedure to configure MVR for the site, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure MVR and click on the Properties button. The VPLS Site (Edit) form opens with the General tab displayed.

5 Click on the Multicast tab.

6 Click on the MVR tab. The General tab is displayed.

7 Configure the parameters:

- Administrative State
- Description
- Use Component Package Policy
- Routing Policy Name

The Administrative State parameter specifies whether a site is an MVR VPLS site.

After the multicast package policy is applied to the MVPLS, the policy is distributed as the routing policy to all MVR-capable MVPLS sites. If you apply another package policy to the site, the new policy is distributed to the site. The previously distributed policy remains on the site.

8 If you deselect the Use Component Package Policy parameter, you must specify a multicast package policy to associate with the MVR VPLS site. Perform one of the following.

a Click on the Select button to specify a multicast package policy. The Select - VPLS Site form opens. Configure the filter criteria to choose a policy. Choose a policy and click on the OK button. The Select - VPLS Site form closes, and the VPLS Site (Create) form refreshes with the policy name.

b Manually enter a multicast package policy name as the Routing Policy Name parameter value.

9 View the VPLS SAPs that use the MVR VPLS site, if required.

i Click on the User MVR SAPs tab.

ii Click on the Search button to list the VPLS SAPs.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The VPLS Site (Edit) form closes.

Procedure 68-18 To configure a GSMP group on a VPLS site

Perform the following procedure to configure a GSMP group on the site, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure a GSMP group and click on the Properties button. The VPLS Site (Edit) form opens with the General tab displayed.

5 Click on the Multicast tab.

6 Click on the GSMP tab.

7 Click on the Create button. The GSMP Group (Create) form opens with the General tab displayed.

8 Configure the following parameters:

- Displayed Name
- Description
- Administrative State
- Keep-Alive (seconds)
- Hold Multiplier
- OAM Administrative State
- Dynamic Topology Discovery

9 Click on the GSMP Group Neighbor tab.

10 Click on the Create button. The GSMP (Create) form opens with the General tab displayed.

11 Configure the following parameters:

- IP Address
- Description
- Administrative State
- Local Address
- Priority Type
- Priority Precedence
- Priority Dscp

The Priority Precedence parameter is configurable when the Priority Type parameter is set to Precedence.

The Priority Dscp parameter is configurable when the Priority Type parameter is set to Dscp.

12 Click on OK button. The GSMP (Create) form closes.

13 Click on OK button. A dialog box appears.

14 Click on the OK button. The GSMP Group (Create) form closes.

15 Click on the OK button. A dialog box appears.

16 Click on the Yes button. The VPLS Site (Edit) form closes.

Procedure 68-19 To configure L2 management interfaces on a VPLS site

Perform the following procedure to configure L2 management interfaces, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure L2 management interfaces and click on the Properties button. The VPLS Site (Edit) form opens with the General tab displayed.

5 Click on the L2 Management Interfaces tab.

6 Click on the Create button. The VPLS L2 Management Interface, Service - Subscriber (Create) form opens with the General tab displayed.

7 Configure the following parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- ARP Timeout (seconds)
- I/F MAC Address

8 Click on the Addresses tab.

9 Click on the Create button. The IP Address, Service - Subscriber (Create) Form opens.

10 Configure the following parameters:

- Address ID
- IP Address
- Prefix Length
- Broadcast Address Format

11 Click on the OK button. A dialog box appears.

12 Click on the OK button. The IP Address, Service - Subscriber (Create) form closes.

13 Click on the OK button. A dialog box appears.

14 Click on the OK button. The VPLS L2 Management Interface, Service - Subscriber (Create) form closes.

15 Click on the OK button. A dialog box appears.

16 Click on the Yes button. The VPLS Site (Edit) form closes.

Procedure 68-20 To configure MLD snooping for a VPLS site

Perform the following procedure to configure MLD snooping for the site, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure MLD snooping and click on the Properties button. The VPLS Site (Edit) form opens with the General tab displayed.

5 Click on the Multicast tab.

6 Click on the MLD Snooping tab.

7 Configure the parameters:

- Administrative State
- Query Interval (seconds)
- Robust count
- Report source address
- Query source address

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button. The VPLS Site (Edit) form closes.

Procedure 68-21 To create a virtual MEP on a VPLS site

Perform the following procedure to create a virtual MEP on a VPLS site, if required. For more information about virtual MEPs, see chapter 78.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to create a virtual MEP and click on the Properties button. The VPLS Site (Edit) form opens with the General tab displayed.

5 Click on the ETH-CFM tab.

6 Configure the Tunnel Fault Notification parameter, if required.

7 Click on the Create button in the Virtual MEP panel. The MEP (Create) form opens.

8 Click on the Select button. The Select Maintenance Entity Group form opens.

9 Choose a MEG from the list.

10 Click on the OK button. The Select Maintenance Entity Group form closes, and the MEG information is displayed on the MEP (Create) form.

11 Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- Description
- MAC Address
- CCM Enabled
- Priority Level for CCM
- Fault Propagation
- CCM Padding Packet Size (Bytes)
- Low-priority Defect

12 As required, configure the Test Generation Options parameters:

- Role
- Use as Test Source
- Use as Test Target



Note — The Role, Use as Test Source, and Use as Test Target parameters are configurable only when you set the Direction parameter to Up.

13 Click on the OK button. The MEP (Create) form closes, and the virtual MEP is created on the site.



Note — After the site is created and is operational, you can open the MEP (Edit) form and view an information field on the General tab that displays the number of Continuously Running Tests currently on the MEP.

14 Click on the OK button. A dialog box appears.

15 Click on the Yes button. The VPLS Site (Edit) form closes.

Procedure 68-22 To configure MVR for MLD on a VPLS site

Perform the following procedure to configure MVR for MLD on the site, if required. The MVR (MLD) tab is configurable depending on the type of device that you are configuring.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure MVR for MLD and click on the Properties button. The VPLS Site (Edit) form opens with the General tab displayed.

5 Click on the Multicast tab.

6 Click on the MVR (MLD) tab. The General tab is displayed.

7 Configure the parameters:

- Administrative State
  The Administrative State parameter specifies whether the site is an MVR VPLS site.
- Description
- Use Component Package Policy
- Routing Policy Name

The Routing Policy Name parameter is configurable when the Use Component Package Policy is disabled.

After a multicast package policy is applied to an MVPLS, the policy is distributed as the routing policy to all MVR-capable MVPLS sites. If you apply another package policy to the site, the new policy is distributed to the site and the previously distributed policy remains on the site.

8 If you deselect the Use Component Package Policy parameter, you must specify a multicast package policy to associate with the MVR VPLS site. Perform one of the following.

- Click on the Select button to specify a multicast package policy. The Select - VPLS Site form opens. Configure the filter criteria to choose a policy. Choose a policy and click on the OK button. The Select - VPLS Site form closes, and the VPLS Site (Create) form refreshes with the policy name.
- Manually enter a multicast package policy name as the Routing Policy Name parameter value.

9 Click on the User MVR SAPs tab to view the VPLS SAPs that use the MVR VPLS site, if required.

- Click on the Search button to list the VPLS SAPs.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The VPLS Site (Edit) form closes.

Procedure 68-23 To configure IGMP host tracking on a VPLS site

Perform the following procedure to configure IGMP host tracking, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure IGMP host tracking and click on the Properties button. The VPLS Site (Edit) form opens with the General tab displayed.

5 Click on the IGMP Host Tracking tab.

6 Configure the parameters:

- Expiry Time (seconds)
- Administrative State

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The VPLS Site (Edit) form closes.

Procedure 68-24 To create a VPLS or MVPLS L2 access interface

Perform this procedure to create a VPLS or an MVPLS L2 access interface.



Caution — The creation of a SAP that uses the same port and encapsulation values as an existing inactive MSAP fails under the following conditions:

- If you try to use the 5620 SAM to create a SAP, the configuration fails and the 5620 SAM displays an error message.
- If you use a CLI to create a SAP in a service other than the service that contains the MSAP, the configuration succeeds but the MSAP is inactive until the regular SAP is deleted. Although the 5620 SAM displays the SAP and MSAP, the MSAP remains inactive and consumes resources.
- If you use a CLI to create a SAP in the service that contains the MSAP, the SAP creation fails.

Alcatel-Lucent recommends that you delete an inactive MSAP from the 5620 SAM if you need to create a regular SAP on the same port using the same encapsulation values. See Procedure 65-34 for more information about deleting MSAPs.



Note 1 — The tabs that are available depend on the NE type on which you are configuring an MVPLS L2 access interface.

Note 2 — If the 7210 SAS-E or 7210 SAS-D sites are connected in a ring network, you must configure an uplink SAP between each pair of 7210 SAS-E or 7210 SAS-D sites.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site to which you want to add the access interface.

For information on adding a GNE service interface to a VPLS service, see Procedure 68-71.

5 Right-click on L2 Access Interfaces and choose Create VPLS L2 Access Interface. The VPLS L2 Access Interface (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Description
- Administrative State

7 Configure the NE-specific parameters, as shown in Table 68-8

Table 68-8 NE-specific parameters

NE	Parameters	Dependencies
7750 SR, 7450 ESS, 7710 SR, 7950 XRS	• Cflowd Type • MC Ring Node • SAP Sub Type • Calling Station ID • Enable Virtual MEP Filter	Set the SAP Sub Type parameter to Regular. Go to step 12. Set the SAP Sub Type parameter to Capture. The VPLS L2 Access Interface (Create) form refreshes to allow the configuration of the Capture SAP. To create a Capture SAP, see Procedure 65-28.
7705 SAR	• PPPoE Circuit ID	No dependencies. Go to step 14.
7210 SAS-D, 7210 SAS-E, 7210 SAS-X	• MC Ring Node	No dependencies. If you are configuring a 7210 SAS-D, 7210 SAS-E, or 7210 SAS-X, go to step 14.

8 On the Split Horizon Group panel, choose an SHG for the interface, if required.

i Click on the Select button in the Split Horizon Group panel. The Select Split Horizon Group Name - VPLS L2 Access Interface form opens.



Note — You must configure an SHG or residential SHG for a VPLS if you plan to create a spoke circuit from this VPLS site to a VLL or another VPLS.

ii Choose an SHG and click on the OK button. The Select Split Horizon Group Name - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form refreshes with the SHG name.

9 Select an application profile for the L2 access interface.

i Click on the Select button beside the Application Profile parameter. The Application Profile String: - VPLS L2 Access Interface form opens.

ii Configure the filter criteria. A list of application profiles appears.

iii Choose an application profile from the list and click on the OK button. The Application Profile String: - VPLS L2 Access Interface form closes and VPLS L2 Access Interface (Create) form refreshes with the application profile information.



Note — The Application Profile String: - VPLS L2 Access Interface service form displays only local profiles on the NE.

10 Associate an AA transit prefix policy with the L2 access interface, if required. Click on the Select button in the Transit Prefix Policy panel to select a policy.



Note 1 — To bind a transit policy to an access interface, a port must already exist on the interface.

Note 2 — You can bind a transit policy to only one access interface or spoke SDP binding per NE.

Note 3 — The transit policy and the application profile must belong to the same application assurance group or partition.

11 Associate a host lockout policy with the L2 access interface, if required. Click on the Select button in the Host Lockout panel to select a policy.

12 Select an operational group for the L2 access interface to join as a member. To select an operational group for the L2 access interface to monitor, go to step 13.

i Click on the Select button beside the Member Group Name parameter. The Select Operational Group - VPLS L2 Access Interface form opens.

ii Configure the filter criteria. A list of operational groups appears.

iii Choose an operational group from the list and click on the OK button. The Select Operational Group - VPLS L2 Access Interface form closes and the VPLS L2 Access Interface (Create) form refreshes with the operational group information.

13 Select an operational group for the L2 access interface to monitor. Perform the following steps.

i Click on the Select button beside the Monitored Group Name parameter. The Select Operational Group - VPLS L2 Access Interface form opens.

ii Configure the filter criteria. A list of operational groups appears.

iii Choose an operational group from the list and click on the OK button. The Select Operational Group - VPLS L2 Access Interface form closes and the VPLS L2 Access Interface (Create) form refreshes with the operational group information.

14 Click on the Port tab.

15 Click on the Select button to choose a port for the L2 access interface. The Select Terminating Port - VPLS L2 Access Interface form opens.



Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

16 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form displays the port information.



Note — If you select an Ethernet Tunnel Endpoint, the Port form is refreshed and an Ethernet Tunnel tab is added.

17 Configure the parameters:

- Outer Encapsulation Value
- Inner Encapsulation Value
- Outer Encapsulation Value (VPI)
- Inner Encapsulation Value (VCI)

When the selected port uses dot1q encapsulation, you can enable the Auto-Assign ID parameter to have the Outer Encapsulation Value parameter automatically assigned. If you choose this, the system assigns the lowest unused encapsulation value.



Note — You can set the Auto-Assign ID parameter to be the default parameter for dot1q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter in the User Preferences form. Choose Application→ User Preferences from the main menu.

If the port you have chosen is an Ethernet Tunnel Endpoint, you will be able to set the Outer Encapsulation Value to 8191. This automatically enables the Ethernet Tunnel Endpoint Control SAP parameter.

If you are configuring the port for an L2 Access Interface in a Control VPLS for an Ethernet ring, the Outer Encapsulation Value and Inner Encapsulation Value parameters for the port in each L2 Access Interface must have the same value as the R-APS Tag (Outer Encapsulation Value) and R-APS Tag (Inner Encapsulation Value) respectively, that you use for the particular path endpoint. This defines the interface as a Control SAP for the Ethernet ring. Refer to Procedure 27-8 for additional information.

The Inner Encapsulation Value is configurable only when the port is an Ethernet or frame relay port with QinQ encapsulation.

The Outer Encapsulation Value (VPI) and Inner Encapsulation Value (VCI) parameters are configurable only when the port is an ATM port.

18 Configure the NE-specific parameters, as shown in Table 68-9

Table 68-9 NE-specific parameters

NE	Parameters	Dependencies
7750 SR, 7450 ESS, 7710 SR, 7705 SAR, 7950 XRS	• Translation • Translation ID	If the port you have chosen is an Ethernet port and uses ATM, dot1q or QinQ encapsulation, you can enable ingress VLAN translation.
7210 SAS-D, 7210 SAS-E, 7210 SAS-M, 7210 SAS-T, 7210 SAS-X	Transit SAP	No dependencies

19 Configure the Ethernet Tunnel Endpoint Control SAP parameter, if required.



Note — Enabling the Ethernet Tunnel Endpoint Control SAP parameter creates the control L2 Access Interface (also known as a Control SAP). It also automatically sets the value of the Outer Encapsulation Value parameter to 8191.

If you are currently creating a same-fate SAP or an L2 Access Interface for an Ethernet ring, the Ethernet Tunnel Endpoint Control SAP parameter must not be enabled.

20 If you are creating this L2 Access Interface for the Control VPLS of an Ethernet ring or for a data service using the ring, configure the ID parameter in the Ethernet Ring Element section to select the required Ethernet Ring Element. Refer to Procedure 27-6 for additional information.

21 Depending on the port that you have chosen, the Egress Multicast Group tab is configurable. Configure the EMG, if required.

i Click on the Egress Multicast Group tab. The Select Egress Multicast Group-L2 Access Interface form opens.

ii Choose an EMG and click on the OK button. The Select Egress Multicast Group-L2 Access Interface form closes, and the Egress Multicast Group tab refreshes with the EMG name.



Note — The Egress Multicast Group-L2 Interface form lists only EMGs that have the same egress filter and encapsulation type as the interface.

22 If the selected port uses FR encapsulation, configure Frame Relay for the interface.

i Click on the Frame Relay tab.

ii Set the FRF-12 Mode parameter to Enabled.

iii Configure the parameters:

- FRF-12 End-To-End Fragment Threshold
- Scheduling Class
- Fragment Interleave



Note — If you select a bundle in step 16, only the Scheduling Class parameter is configurable.

23 Configure the Enable Split Horizon parameter.



Note — If you are configuring the control SAP for a 7210 SAS-M Uplink, Release 4.0 R3 or later, to be used as an interconnected NE in an Ethernet sub-ring, you must enable the Enable Split Horizon parameter.

24 If you are configuring an NE other than a 7210 SAS-D or 7210 SAS-E, click on the General tab. Otherwise, go to step 26.

25 Configure the parameters in the ETH-CFM MIP panel:

- MIP
- MIP MAC Address



Note 1 — The MIP and MIP MAC Address parameters are configurable only when a port is assigned to the interface.

Note 2 — You cannot configure MIPs on SPB-enabled SAP and spoke SDP bindings. See "SPB in VPLS" for more information about SPB.

26 Assign ingress and egress ACL filters to the interface, if required.

i Click on the ACL tab.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - VPLS L2 Access Interface form opens.

iii Choose an ingress ACL filter and click on the OK button. The Select Ingress Filter - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form refreshes with the ingress ACL filter name.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - VPLS L2 Access Interface form opens.

v Choose an egress ACL filter and click on the OK button. The Select Egress Filter - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form refreshes with the egress ACL filter name.

vi Click on the Select button in the IPv6 Ingress Filter panel to choose an IPv6 ingress ACL filter. The Select IPv6 Ingress Filter - VPLS L2 Access Interface form opens.



Note — When you configure IPv6 ingress ACL filters on a 7210 SAS-E Release 5.0 R3 or later, you must configure the system resource profile appropriately on the device. See "System resource profile" in section 8.5 and Procedure 13-20 for more information.

vii Choose an IPv6 ingress ACL filter and click on the OK button. The Select IPv6 Ingress Filter - VPLS L2 Access Interface form closes and the VPLS L2 Access Interface (Create) form reappears with the IPv6 ingress ACL filter information displayed.

viii Click on the Select button in the IPv6 Egress Filter panel to choose an IPv6 egress ACL filter. The Select IPv6 Egress Filter - VPLS L2 Access Interface form opens.

ix Choose an IPv6 egress ACL filter and click on the OK button. The Select IPv6 Egress Filter - VPLS L2 Access Interface form closes and the VPLS L2 Access Interface (Create) form reappears with the IPv6 egress ACL filter information displayed.

27 Assign an accounting policy to the interface, if required.

i Click on the Accounting tab.

ii Click on the Select button to choose an accounting policy. The Select Accounting Policy - VPLS L2 Access Interface form opens.

iii Choose an accounting policy and click on the OK button. The Select Accounting Policy - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form refreshes with the accounting policy name.

iv Configure the Collect Accounting Statistics parameter.

v If you are configuring statistics collection for a 7210 SAS, configure the following parameters. Otherwise, go to step 28.

- Enable Egress Packets Forwarding
- Ingress Counter Mode
- Ingress Counter Type

28 Assign a time of day suite to the interface, if required.

i Click on the TOD Suite tab.

ii Click on the Select button beside the Name parameter. The Select Time Of Day Suite - VPLS L2 Access Interface form opens.

iii Choose a time of day suite and click on the OK button. The Select Time Of Day Suite - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form refreshes with the time of day suite name.



Note 1 — You cannot assign a ToD suite to a L2 access interface if accounting statistics collection is enabled on the L2 access interface. You must first disable the Collect Accounting Statistics parameter in step 27.

Note 2 — SapEgrQosPlcyStats and SapIngQosPlcyStats statistics will only be collected if a Time Of Day Suite is applied on the SAP.

29 The ATM tab is configurable when the interface port is an ATM port. Specify OAM functionality and assign ingress and egress ATM policies to the interface, if required. Otherwise, go to step 30.

i Click on the ATM tab.

ii Configure the parameters:

- AAL5 Encapsulation
- ATM OAM Alarm Cell Handling

iii Click on the Select button in the Ingress ATM Policy panel to choose an ingress ATM policy. The Select Ingress ATM Policy - ATM Configuration form opens.

iv Choose an ingress ATM policy and click on the OK button. The Select Ingress ATM Policy - ATM Configuration form closes, and the VPLS L2 Access Interface (Create) form refreshes with the ingress ATM policy name.

v Click on the Select button in the Egress ATM Policy panel to choose an egress ATM policy. The Select Egress ATM Policy - ATM Configuration form opens.

vi Choose an egress ATM policy and click on the OK button. The Select Egress ATM Policy - ATM Configuration form closes, and the VPLS L2 Access Interface (Create) form refreshes with the egress ATM policy name.

30 Click on the MIPs tab.

31 Perform one or more of the following, if required:

a Click on the Search button to list available MIPs.

b View the current status of a specific MIP entry.

i Select a MIP from the list.

ii Click on the Properties button to display the MIP information.

c Click on the Resync button to resync the latest MIPs configured on the NE.

32 Specify the queue overrides.

i Click on the Override Policy Items tab.



Note — The Override Policy Items tab contains a number of tabs. However, the tabs that are displayed depend on the port type that you have chosen for this interface.

- If you configured a non-HSMDA port, then the Access Ingress Queues, Access Egress Queues, Ingress Policer, and Egress Policer tabs are active.
- If you configured an HSMDA port, then the Access Ingress Queues, Access Egress HSMDA Queues and Ingress Policer tabs are active.

ii Set the queue overrides, as described in Procedure 43-42.

33 Click on the OK button. The VPLS L2 Access Interface (Create) form closes and a dialog box appears.

34 Click on the OK button. The VPLS Service form reappears.

35 Repeat steps 5 to 34 for each additional access interface that you want to create.

36 To configure BPDU Termination, STP, and FIB parameters for the L2 access interface, perform Procedure 68-27.

37 To assign a DoS protection policy or DDoS protection policy to the L2 access interface, perform Procedure 68-28.

38 To configure residential subscriber management on the L2 access interface, perform Procedure 68-29.

39 To configure an Ethernet tunnel on the L2 access interface, perform Procedure 68-30.

40 To configure a redundant VLAN range on the L2 access interface, perform Procedure 68-31.

41 To configure IGMP snooping on the L2 access interface, perform Procedure 68-32.

42 To configure the ARP host for the L2 access interface, perform Procedure 68-33.

43 To configure DHCP on the L2 access interface, perform Procedure 68-34.

44 To configure MVR for the L2 access interface, perform Procedure 68-35.

45 To configure anti-spoofing on the L2 access interface, perform Procedure 68-36.

46 To associate a MEP to the L2 access interface, perform Procedure 68-37.

47 To assign an ANCP policy to the L2 access interface, perform Procedure 68-38.

48 To configure PIM snooping on the L2 access interface, perform Procedure 68-39.

49 To configure MLD snooping on the L2 access interface, perform Procedure 68-40.

50 To configure MVR (MLD) on the L2 access interface, perform Procedure 68-41.

51 To configure custom object attributes for AA reporting to the 5670 RAM on the L2 access interface, perform Procedure 68-42.

Procedure 68-25 To assign ingress and egress QoS policies to an L2 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface and choose Properties. The VPLS L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the QoS tab.

8 To configure a 7210 SAS NE, perform the following steps. Otherwise, go to step 13.



Note — You can only assign policies and configure parameters for 7210 SAS NEs when the system resource profile is appropriately configured for the device. See "System resource profile" in chapter 8.

9 Click on the Select button in the 7210 Specific panel to choose a SAS ingress policy. The Select SAS Ingress Policy - VPLS L2 Access Interface form opens.

10 Choose a SAS ingress policy and click on the OK button. The Select SAS Ingress Policy - VPLS L2 Access Interface form closes and the information is displayed.



Note — To support H-metering, you must choose a SAS ingress policy with all meter rate modes set to trtcm2.

11 Configure the following parameters in the Aggregate Rate Limit panel:

- Ingress Meter
- Ingress Meter Rate (kbps)
- Ingress Meter Burst
- Aggregate Shaper CIR Rate (kbps)
- Aggregate Shaper PIR Rate (kbps)



Note 1 — You can configure the Ingress Meter parameter only during SAP creation on the 7210 SAS-M, 7210 SAS-T, or 7210 SAS-X. The parameter must be set to true to support H-metering.

Note 2 — You can configure the Ingress Meter Rate (kbps) and Ingress Meter Burst parameters only after SAP creation on the 7210 SAS-M, 7210 SAS-T, or 7210 SAS-X.

12 Go to step 31.

13 Configure the Ingress Match QinQ Dot1P parameter.

The Ingress Match QinQ Dot1P parameter is configurable only when the encapsulation type of the port is dot1q, BCP dot1q, or QinQ.

14 Click on the Select button in the Ingress Policy panel to choose an ingress QoS policy. The Select Ingress Policy - VPLS L2 Access Interface form opens.

15 Choose an ingress QoS policy and click on the OK button. The Select Ingress Policy - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form refreshes with the ingress QoS policy name.



Note — If you choose an access ingress policy which has a forwarding class mapped to an ingress queue group, you must ensure that port that you are configuring for the VPLS L2 access interface has the access ingress queue group with the same name created on it.

See Procedure 16-1 for more information about how to configure Ethernet ports. See chapter 42 for more information about queue group template policies.

16 Click on the Select button in the Forwarding Plane Redirect panel to choose an ingress queue group template policy. The Select Forwarding Plane Queue Group Instance form opens.

17 Choose a policy from the list and click on the OK button. The Select Forwarding Plane Queue Group Instance form closes. The VPLS L2 Access Interface (Create) form refreshes with the Ingress Queue Group Template Policy information displayed.

18 Configure the Instance ID parameter.

19 Configure the Egress Mark QinQ Top Bits Only parameter.

The Egress Mark QinQ Top Bits Only parameter is configurable only when the encapsulation type of the port is dot1q, BCP dot1q, or QinQ.

20 Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - VPLS L2 Access Interface form opens.

21 Choose an egress QoS policy and click on the OK button. The Select Egress Policy - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form refreshes with the egress QoS policy name.



Note — If you choose an access egress policy which has a forwarding class mapped to an egress queue group, you must ensure that port that you are configuring for the VPLS L2 access interface has the access egress queue group with the same name created on it.

See Procedure 16-1 for more information about how to configure Ethernet ports. See chapter 42 for more information about queue group template policies.

22 Click on the Select button in the Port Redirect panel to choose an Egress Queue Group Template Policy, if required. The Select Egress Queue Group Template Policy form opens.



Note — Selecting an Egress Queue Group Template Policy here permits the redirection of Ethernet traffic packets to a queue ID specified in the SAP's egress port queue group. The following properties and restrictions apply:

- If an Egress Queue Group Template Policy is specified here, the policy must have port redirection enabled.
- You cannot use policy-based redirection with the queue group when the SAP has SAP-based redirection enabled.
- Port access egress redirection is only supported on Ethernet/LAG ports. It is not supported on SAPs bound on non-Ethernet, Eth-tunnel, or CCAG ports.
- Supported ports include access, hybrid, and HSMDA.
- Queue groups can be applied to SAPs that incorporate LAGs. The LAGs can include port members from just a single card or from multiple cards.
- If you edit a LAG incorporated by the SAP, you cannot remove the last LAG member if a queue group reference exists to the containing SAP.
- You cannot add a secondary LAG member that has a queue group mismatch with primary LAG member.

23 Choose an Egress Queue Group Template Policy and click on the OK button. The Select Egress Queue Group Template Policy form closes, and the VPLS L2 Access Interface (Create) form refreshes with the Egress Queue Group Template Policy information displayed.

24 If you are configuring an L2 access interface for a 7710 SR or 7705 SAR, or if the port you selected in step 16 of Procedure 68-24 is not an HSMDA port, go to step 7 of Procedure 68-26.

25 Configure the Packet Byte Offset (bytes) parameter, if required. Before you can configure the parameter, you must select the associated Override check box.

26 Click on the Select button in the Egress HSMDA Override panel to choose a WRR policy. The Select WRR Policy form opens.

27 Choose a WRR policy and click on the OK button. The Select WRR Policy form closes and the VPLS L2 Access Interface (Create) form reappears with the WRR policy information displayed.

28 Click on the Select button in the Egress HSMDA Override panel to choose an HSMDA egress secondary shaper policy. The Select Secondary Shaper form opens.

29 Choose a secondary shaper and click on the OK button. The Select Secondary Shaper form closes and the VPLS L2 Access Interface (Create) form reappears with the secondary shaper information displayed.

30 Configure the parameters:

- Use Shared Queue
- Use Multipoint Shared Queue

31 Click on the OK button. The VPLS L2 Access Interface (Edit) form closes and a dialog box appears.

32 Click on the Yes button. The VPLS Service (Edit) form reappears.

33 Close the VPLS Service (Edit) form.

Procedure 68-26 To configure scheduling on an L2 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click the Search button. A list of services appears.

3 Choose a VPLS and click the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click the L2 access interface and choose Properties. The VPLS L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click the Schedulers tab.



Note — For the 7210 SAS-X, the port is enabled only when you select the SAP based type in the Egress Scheduler Mode.

8 To configure scheduling on a 7705 SAR site, perform the following steps. Otherwise, go to step 9.



Note 1 — For the 7705 SAR, scheduler behavior is determined by the scheduler mode, which is 4-Priority by default. You can only configure the Egress and Ingress Aggregate Rate Limit parameters when the Scheduler Mode parameter is set to 16-Priority. You can set the Scheduler Mode to 16-Priority only when the port is on an MDA that supports 16-Priority. See the 7705 SAR documentation for more information.

Note 2 — If you change the Scheduler Mode parameter from 16-Priority to 4-Priority, the 5620 SAM automatically restores the default settings for the Egress Aggregate Rate Limit and Ingress Aggregate Rate Limit panels when you click on the Apply or OK button.

i In the Egress Scheduler panel, configure the Scheduler Mode parameter.

ii In the Ingress Scheduler panel, configure the Scheduler Mode parameter.

iii If you set the Scheduler Mode parameter to 16-Priority in the Egress Scheduler panel or Ingress Scheduler panel, configure the parameters in the Egress Aggregate Rate Limit panel and Ingress Aggregate Rate Limit panel, as required. Otherwise, go to step 42.

- Assign Aggregate Rate Limit
- Aggregate Rate Limit (kbps)
- Assign Aggregate CIR
- Aggregate CIR (kbps)

iv Go to step 42.

9 If you are applying an aggregation scheduler policy to the interface, set the Aggregation parameter to On. Otherwise, go to step 13.



Note — You cannot specify an access scheduler policy if the port you selected in step 16 of Procedure 68-24 is an HSMDA port. Go to step 42.

10 Click the Select button in the Aggregation Scheduler panel to choose an aggregation scheduler. The Select Aggregation Scheduler - VPLS L2 Access Interface form opens.

11 Choose an aggregation scheduler and click the OK button. The Select Aggregation Scheduler - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form refreshes with the aggregation scheduler information displayed.

12 Go to step 42.

13 Specify that an aggregation scheduler policy is not being applied to the interface. Set the Aggregation parameter to Off.

Note — The Aggregation parameter is not configurable if the port you selected in step 16 of Procedure 68-24 is an HSMDA port.

14 Click the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - VPLS L2 Access Interface form opens.

15 Choose an ingress scheduler and click the OK button. The Select Ingress Scheduler - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Edit) form refreshes with the ingress scheduler information displayed.

16 Configure the parameters:

- Aggregate Rate Limit (kbps)
- Frame-Based Accounting

Note 1 — The Aggregate Rate Limit (kbps) and Frame-Based Accounting parameters are configurable only when there is no scheduler specified in the Egress Scheduler panel.

Note 2 — The Frame-Based Accounting parameter is not configurable if the port you selected in step 16 of Procedure 68-24 is an HSMDA port.

Note 3 — You cannot specify an egress scheduler when the Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

17 Click the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Policer Control Policy form opens.

18 Choose a policer control policy and click the OK button. The Select Policer Control Policy form closes and the VPLS L2 Access Interface (Edit) form reappears with the ingress policer control policy information displayed.

19 Click the Create button in the Ingress Policer Control Override panel. The Ingress Policer Control Override (Create) form opens, with the General tab displayed.

20 Configure the parameters:

- Maximum Frame Based Bandwidth (kbps)
- Minimum Separation Buffer Space (bytes)

21 A message is displayed. Click OK.

22 Click the Level Override Policy Items tab.

23 Select an item from the list and click Properties. The Ingress Policy Policer Level Override form opens, with the General tab displayed.

24 Click the Override tab.

25 Configure the override for the Maximum Cumulative Buffer Space (bytes) parameter.

26 Click OK. The Ingress Policy Policer Level Override form closes.

27 Click OK. The Ingress Policer Control Override (Create) form closes.

28 If the port you selected step 16 of Procedure 68-24 is an HSMDA port, go to step 42.

29 Click the Select button in the Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - VPLS L2 Access Interface form opens.

30 Choose an egress scheduler and click the OK button. The Select Egress Scheduler - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form refreshes with the egress scheduler information displayed.

31 Click the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Policer Control Policy form opens.

32 Choose a policer control policy and click the OK button. The Select Policer Control Policy form closes and the VPLS L2 Access Interface (Create) form reappears with the egress policer control policy information displayed.

33 Click the Create button in the Egress Policer Control Override panel. The Egress Policer Control Override (Create) form opens, with the General tab displayed.

34 Configure the parameters:

- Maximum Frame Based Bandwidth (kbps)
- Minimum Separation Buffer Space (bytes)

35 A message is displayed. Click OK.

36 Click the Level Override Policy Items tab.

37 Select an item from the list and click Properties. The Egress Policy Policer Level Override form opens, with the General tab displayed.

38 Click the Override tab.

39 Configure the override for the Maximum Cumulative Buffer Space (bytes) parameter.

40 Click OK. The Ingress Policy Policer Level Override form closes.

41 Click OK. The Ingress Policer Control Override (Create) form closes.

42 Click the OK button. The VPLS L2 Access Interface (Edit) form closes and a dialog box appears.

43 Click the Yes button. The VPLS Service (Edit) form reappears.

44 Close the VPLS Service (Edit) form.

Procedure 68-27 To configure BPDU Termination, STP, and FIB parameters for the VPLS L2 access interface

Perform the following procedure to configure BPDU Termination, STP, and FIB parameters for the interface, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface on which you want to configure BPDU Termination, STP and FIB parameters and choose Properties. The VPLS L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Forwarding Control tab. Depending on the device being configured, the BPDU Termination tab is displayed. Otherwise, go to step 10.

8 Configure the parameters:

- L2 Protocol Termination
- BPDU Translation

When the L2 Protocol Termination parameter is set to Enabled, a list of L2PT protocols is displayed. Select all that are required.

9 Configure the NE-specific parameters, as shown in Table 68-10

Table 68-10 NE-specific parameters

NE	Parameters	Dependencies
7750 SR, 7450 ESS, 7710 SR, 7950 XRS	• Force L2PT on Managed L2 Access Interface	The Force L2PT on Managed L2 Access Interface parameter is only available for MVPLS L2 access interfaces. When the Force L2PT on Managed L2 Access Interface parameter is set to Enabled, a list of L2PT protocols is displayed. Select all that are required.
7705 SAR	No NE-specific parameters.	

10 Click on the STP tab.

11 Configure the parameters:

- Path Cost
- Port Number
- Priority
- Edge Port
- Edge Capability Detection
- Link Type
- Root Guard
- Administrative State

12 Click on the FIB tab.

13 Configure the parameters:

- Aging Enabled
- Learning Enabled
- Maximum Entries
- Limit Mac Move
- Discard Unknown Source

14 Configure the NE-specific parameters, as shown in Table 68-9

Table 68-11 NE-specific parameters

NE	Parameters	Dependencies
7750 SR, 7450 ESS, 7710 SR, 7950 XRS	• Restrict Protected Source • Restrict Protected Source Action • Restrict Unprotected Destination • Auto Learn MAC Protect • Limit Mac Move Level	The Restrict Protected Source Action parameter is configurable only when the Restrict Protected Source is set to true.
7705 SAR	• Limit Mac Move Level	No dependencies.
7210 SAS-D, 7210 SAS-X, 7210 SAS-E	No NE-specific parameters.	

15 If you are creating an MVPLS to run MSTP, the MST Instances tab is configurable. Otherwise, go to step 21.

16 Click on the MST Instances tab to edit a SAP MST instance.

17 Select an MST instance and click on the Properties button.

18 The L2 Access Interface MST Instance (Edit) form opens. Configure the parameters:

- Path Cost
- Priority

19 Click on the OK button to close the L2 Access Interface MST Instance (Edit) form. A dialog box appears.

20 Click on the OK button. The L2 Access Interface (Edit) form refreshes with the new MST instance.

21 Click on the OK button. The VPLS L2 Access Interface (Edit) form closes and a dialog box appears.

22 Click on the Yes button. The VPLS Service (Edit) form reappears.

23 Close the VPLS Service (Edit) form.

Procedure 68-28 To assign a DoS protection policy or DDoS protection policy to the VPLS L2 access interface

Perform the following procedure to assign a DoS protection policy to the interface, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface on which you want to assign a DoS protection policy or DDoS protection policy and choose Properties. The VPLS L2 Access Interface (Edit) form opens with the General tab displayed.



Note — A default DoS protection policy is automatically assigned to the interface.

7 Click on the Security tab.

8 Click on the Select button in the NE DoS Protection panel and select a DoS protection policy from the Select NE DoS Protection form.

9 Click on the Select button next to the NE DDoS Protection Policy field and select a DDoS protection policy from the Select NE DDoS Protection Policy form.

10 Configure the MAC Monitoring parameter.

11 Configure the Ethernet CFM Monitor Flags parameter.

12 Click on the OK button. The VPLS L2 Access Interface (Edit) form closes and a dialog box appears.

13 Click on the Yes button. The VPLS Service (Edit) form reappears.

14 Close the VPLS Service (Edit) form.

Procedure 68-29 To configure residential subscriber management for the VPLS L2 access interface

Perform the following procedure to configure residential subscriber management for the interface, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface on which you want to configure residential subscriber management and choose Properties. The VPLS L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Subscriber Management tab. The Host Connectivity tab is displayed.

8 Select the SHCV Enabled parameter to enable SHCV, if required. Otherwise, go to step 10.

9 Configure the parameters:

- SHCV Interval (minutes)
- SHCV Source
- SHCV Source MAC Address
- SHCV Action
- SHCV Retry Timeout (seconds)
- SHCV Retry Count

10 Click on the IGMP Host Tracking tab.

11 Click on the Select button to choose the import policy used to filter IGMP packets. The Select SapIgmpHostTracking form opens.

12 Configure the filter criteria and click on the Search button. A list of import policies appears.

13 Choose a policy and click on the OK button. The selected import policy name appears.

14 Configure the parameters:

- Expiry Time (seconds)
- Maximum Number of Groups
- Maximum Number of Sources per Group
- Maximum Number of Group Sources per Group
- Disable Router Alert Check

15 Click on the Profiles tab.

16 Configure the parameters:

- Admin Status
- Service Model
- Subscriber Limit
- Default Subscriber Identification Type
- Default Subscriber ID
- Default Intermediate Destination Id Type
- Default Intermediate Destination Id
- Profiled Traffic only
- Non-Subscriber Traffic Identification
- LAG link selection

17 Click on the Select button in the Default Subscriber Profile panel to choose a default subscriber profile for the interface, if required. The Select Default Subscriber Profile form opens with the list of available subscriber profiles displayed.

18 Choose a subscriber profile and click on the OK button. The Select Default Subscriber Profile form closes, and the subscriber profile name appears in the Default Subscriber Profile panel.

19 Click on the Select button in the Default SLA Profile panel to choose a Default SLA profile for the SAP, if required. The Select Default SLA Profile form opens with the list of available SLA profiles displayed.

20 Choose an SLA profile and click on the OK button. The Select Default SLA Profile form closes, and the SLA profile name appears in the Default SLA Profile panel.

21 Click on the Select button in the Subscriber Identification Policy panel to choose a subscriber identification policy for the SAP, if required. The Select Subscriber Identification Policy form opens with the list of available subscriber identification policies displayed.

22 Choose a subscriber identification policy and click on the OK button. The Select Subscriber Identification Policy form closes, and the subscriber identification policy name appears in the Subscriber Identification Policy panel.

23 Click on the Select button in the Default Application Profile panel to choose a default application profile for the SAP, if required. The Select Default Application Profile form opens with the list of application profiles on the NE displayed.

24 Choose an application profile and click on the OK button. The Select Default Application Profile form closes, and the application profile name appears in the Default Application Profile panel.

25 Click on the Select button in the Non-Subscriber Traffic Subscriber Profile panel to choose a non-subscriber subscriber profile for the SAP, if required. The Select Non-Subscriber Traffic Subscriber Profile form opens with the list of available subscriber profiles displayed.

26 Choose a subscriber profile and click on the OK button. The Select Non-Subscriber Traffic Subscriber Profile form closes, and the subscriber profile name appears in the Non-Subscriber Traffic Subscriber Profile panel.

27 Click on the Select button in the Non-Subscriber Traffic SLA Profile panel to choose a Non-Subscriber Traffic SLA profile for the SAP, if required. The Select Non-Subscriber Traffic SLA Profile form opens with the list of available SLA profiles displayed.

28 Choose an SLA profile and click on the OK button. The Select Non-Subscriber Traffic SLA Profile form closes, and the SLA profile name appears in the Non-Subscriber Traffic SLA Profile panel.

29 Click on the Select button in the Non-Subscriber Traffic Application Profile panel to choose a non-subscriber traffic application profile for the SAP, if required. The Select Non-Subscriber Traffic Application Profile form opens with the list of application profiles on the NE displayed.

30 Choose an application profile and click on the OK button. The Select Non-Subscriber Traffic Application Profile form closes, and the application profile name appears in the Non-Subscriber Traffic Application Profile panel.

31 Click on the Host Tracking Info tab to view a list of hosts that are being tracked on this L2 access interface.

32 Click on the OK button. The VPLS L2 Access Interface (Edit) form closes and a dialog box appears.

33 Click on the Yes button. The VPLS Service (Edit) form reappears.

34 Close the VPLS Service (Edit) form.

Procedure 68-30 To configure an Ethernet tunnel on a VPLS L2 access interface

If you are creating a fate-sharing Ethernet Tunnel Endpoint SAP—or same-fate SAP—perform the following procedure to configure an Ethernet tunnel.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface on which you want to configure the ethernet tunnel and choose Properties. The VPLS L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Ethernet Tunnel tab.

8 Click on the Create button. The Ethernet Tunnel (Create) form opens.

9 Configure the parameters:

- Path ID
- Tag (Outer Encapsulation Value)
- Tag (Inner Encapsulation Value)

10 Click on the OK button. A dialog box appears.

11 Click on the OK button. The VPLS L2 Access Interface (Create) form refreshes with the Ethernet Tunnel entry.

12 Click on the OK button. The VPLS L2 Access Interface (Edit) form closes and a dialog box appears.

13 Click on the Yes button. The VPLS Service (Edit) form reappears.

14 Close the VPLS Service (Edit) form.

Procedure 68-31 To configure a redundant VLAN range on a VPLS L2 access interface

Perform the following procedure to configure a redundant VLAN range, if required.



Note — If an MVPLS site has SAPs that manage traffic on the associated VPLS SAPs, you must define a redundant VLAN range during SAP creation. The redundant VLAN range defines the range of VC IDs for VPLS SAPs that the MVPLS manages.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface on which you want to configure a redundant VLAN range and choose Properties. The VPLS L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Redundancy tab.

8 Click on the Create button. The RedundantVlanRange (Create) form opens.

9 Configure the parameters:

- Min VLAN ID
- Max VLAN ID

10 Click on the OK button. A dialog box appears.

11 Click on the OK button. The VPLS L2 Access Interface (Edit) form refreshes with the redundant VLAN range entry.

12 Click on the OK button. The VPLS L2 Access Interface (Edit) form closes and a dialog box appears.

13 Click on the Yes button. The VPLS Service (Edit) form reappears.

14 Close the VPLS Service (Edit) form.

Procedure 68-32 To configure IGMP snooping for the VPLS L2 access interface

Perform the following procedure to configure IGMP snooping for the interface, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface on which you want to configure IGMP snooping and choose Properties. The VPLS L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the IGMP Snooping tab. The General tab is displayed.

8 Configure the parameters:

- Import Policy
- Fast Leave
- Multicast Router Attached
- Send Queries
- General Query Interval (seconds)
- Maximum Response Interval (seconds)
- Robust count
- IGMP Version
- Last Member Query Interval (tenths of seconds)
- Maximum Number of Groups
- Maximum Number of Sources per Group
- Maximum Number of Group Sources per Group

The General Query Interval (seconds), Maximum Response Interval (seconds), Robust count, and IGMP Version parameters are configurable when the Send Queries parameter is enabled.

9 Configure the NE-specific parameters, as shown in Table 68-12

Table 68-12 NE-specific parameters

NE	Parameters	Dependencies
7750 SR, 7450 ESS, 7710 SR, 7950 XRS	• Disable Router Alert Check	No dependencies.
7210 SAS	No NE-specific parameters.	
7705 SAR	No NE-specific parameters.	
OS 9700E, OS 9800E	No NE-specific parameters.	

10 If you are configuring a 7750 SR, 7450 ESS, 7710 SR, or 7950 XRS, click on the Select button in the Multicast CAC Policy panel to choose a multicast CAC policy, if required. The Select Multicast CAC Policy form opens with the list of available multicast CAC policies displayed. Otherwise, go to step 13.

11 Choose a multicast CAC policy and click on the OK button. The Select Multicast CAC Policy form closes and the multicast CAC policy information appears on the VPLS L2 Access Interface (Create) form.

12 Configure the parameters:

- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)
- Constraint Admin State

13 Click on the Static Mcast Group tab to configure a static multicast group, if required.

14 Click on the Create button. The Access Interface Igmp Snooping Mcast Group Display (Create) form opens.

15 Configure the parameters:

- Group Address
- Source Address

16 Click on the Apply button if you want to create additional entries. A dialog box appears. Otherwise, go to step 19.

17 Click on the OK button.

18 Repeat steps 14 to 16 to create an additional entry, if required.

19 Click on the OK button. A dialog box appears.

20 Click on the OK button. The Static Mcast Group tab refreshes with the new multicast group entries.

21 If you are configuring a 7750 SR, 7450 ESS, 7710 SR, or 7950 XRS, click on the LAG Port Down tab. Otherwise, go to step 27

22 Click on the Create button. The LAG Port Down (Create) form opens.

23 Configure the parameters:

- Number of Ports Down
- Level ID

24 Click on the Levels tab.

25 Click on the Create button. The Multicast CAC Level (Create) form opens.

26 Configure the parameters:

- Level ID
- Bandwidth (kbps)

27 Click on the OK button. The VPLS L2 Access Interface (Edit) form closes and a dialog box appears.

28 Click on the Yes button. The VPLS Service (Edit) form reappears.

29 Close the VPLS Service (Edit) form.

Procedure 68-33 To configure the ARP host for the VPLS L2 access interface

Perform the following procedure to configure the ARP host for the interface, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface on which you want to configure the ARP host and choose Properties. The VPLS L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the ARP Host Configuration tab.

8 Configure the parameters:

- Administrative State
- ARP Host Limit
- Minimum Authentication Interval (minutes)

9 Click on the OK button. The VPLS L2 Access Interface (Edit) form closes and a dialog box appears.

10 Click on the Yes button. The VPLS Service (Edit) form reappears.

11 Close the VPLS Service (Edit) form.

Procedure 68-34 To configure DHCP for the VPLS L2 access interface

Perform the following procedure to configure DHCP for the interface, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface on which you want to configure DHCP and choose Properties. The VPLS L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the DHCP tab. The General tab is displayed.

8 Configure the parameters:

- Administrative State
- Description
- Snooping
- Circuit ID
- Remote ID
- Remote ID String
- Vendor Specific Options
- Vendor String

The Remote ID String parameter is configurable when the Remote ID parameter is set to Remote IDString.

9 Configure the NE-specific parameters, as shown in Table 68-13

Table 68-13 NE-specific parameters

NE	Parameters	Dependencies
7750 SR, 7450 ESS, 7710 SR	• Enable • Enable Lease Populate • Action	The Enable Lease Populate parameter is configurable when the Enable parameter is enabled.
7210 SAS	No NE-specific parameters.	
7705 SAR	No NE-specific parameters.	
OS 9700E, OS 9800E	No NE-specific parameters.	

10 Depending on the type and release of the device that you are configuring, the Subscriber Authentication Policy panel appears. Otherwise, go to step 14.

11 Click on the Select button in the Subscriber Authentication panel to choose a subscriber authentication policy. The Select Subscriber Authentication Policy - L2 Access I/F DHCP Relay Config form opens.

12 Click on the Search button. A list of subscriber authentication policies appears.

13 Choose a subscriber authentication policy and click on the OK button. The Select Subscriber Authentication Policy - L2 Access I/F DHCP Relay Config form closes, and the VPLS L2 Access Interface (Create) form refreshes with the subscriber authentication policy name.

14 Click on the Server tab to configure the VPLS L2 access interface proxy server.



Note — You can configure a VPLS L2 access interface proxy server on a 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, 7210 SAS-X 24F 2XFP, 7450 ESS, 7710 SR, or 7750 SR.

15 Configure the parameters:

- Administrative State
- Emulated Server IP Address
- Lease Time
- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time RADIUS Override

The Number of Days, Number of Hours, Number of Minutes, Number of Seconds, and Lease Time RADIUS Override parameters are configurable only when the Lease Time parameter is set to Specified Time Period.

16 Click on the OK button. The VPLS L2 Access Interface (Edit) form closes and a dialog box appears.

17 Click on the Yes button. The VPLS Service (Edit) form reappears.

18 Close the VPLS Service (Edit) form.

Procedure 68-35 To configure MVR for a VPLS L2 access interface

Depending on the type of device that you are configuring, the MVR tab is configurable. Perform the following procedure to configure MVR for the SAP, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface on which you want to configure MVR and choose Properties. The VPLS L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the MVR tab.

8 Click on the Select button in the Source MVR VPLS panel to associate an MVR VPLS with the SAP. The Select Source MVR VPLS form opens.

9 Choose a source MVR VPLS and click on the OK button. The Select Source MVR VPLS closes, and the VPLS L2 Access Interface (Edit) form refreshes with the source MVR VPLS information.

10 Click on the Select button in the Proxy MVR SAP panel to choose a proxy MVR SAP to which the multicast traffic will be sent. The Select Proxy MVR SAP form opens.

11 Choose a proxy MVR SAP and click on the OK button. The Select Proxy MVR SAP form closes, and the VPLS L2 Access Interface (Edit) form refreshes with the proxy MVR SAP information.



Note — If the SAP already has an MVR proxy SAP or is the MVR proxy SAP of another SAP, the SAP cannot be an MVR proxy SAP.

12 Click on the OK button. The VPLS L2 Access Interface (Edit) form closes and a dialog box appears.

13 Click on the Yes button. The VPLS Service (Edit) form reappears.

14 Close the VPLS Service (Edit) form.

Procedure 68-36 To configure anti-spoofing filters for a VPLS L2 access interface

Perform the following procedure to configure anti-spoofing filters for the interface, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface on which you want to configure anti-spoofing filters and choose Properties. The VPLS L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Anti-Spoofing tab.

8 Configure the MAC Pinning parameter.

9 Configure the NE-specific parameters, as shown in Table 68-14

Table 68-14 NE-specific parameters

NE	Parameters	Dependencies
7750 SR, 7450 ESS, 7710 SR	• Anti-Spoofing • ARP Reply Agent	The ARP Reply Agent parameter is configurable only when an IP address is specified for the static hosts on the SAP.
7210 SAS-D, 7210 SAS-E, 7210 SAS-M, 7210 SAS-X	No NE-specific parameters.	
7705 SAR	No NE-specific parameters.	
OS 9700E, OS 9800E	No NE-specific parameters.	

10 Click on the Static Hosts tab to configure a static subscriber host entry for each subscriber host that is not managed by DHCP.

11 Click on the Create button. The Access Interface Anti-Spoofing Static Host Display (Create) form opens.

12 Configure the parameters:

- IP Address
- MAC Address
- Subscriber Identification
- Use SAP ID as Subscriber ID
- ANCP String
- Intermediate Destination ID



Note — You must specify at least one IP address or MAC address for each static host. The values that are specified for the Anti-Spoofing and ARP Reply Agent parameters determine the type of address entry that is required for the static host. For example, if you set the Anti-Spoofing parameter to Source Ip Addr, you must specify at least the IP address for the static host.

13 Configure residential subscriber management for the static host, if required.

14 Click on the Select button in the Subscriber Profile panel to choose a subscriber profile for the static host, if required. The Select Subscriber Profile - AntiSpoofingStaticHosts form opens with the list of available subscriber profiles displayed. Otherwise, go to step 16.

15 Choose a subscriber profile and click on the OK button. The Select Subscriber Profile - AntiSpoofingStaticHosts form closes, and the subscriber profile name appears in the Subscriber Profile panel.

16 Click on the Select button in the SLA Profile panel to choose an SLA profile for the static host, if required. The Select SLA Profile - AntiSpoofingStaticHosts form opens with the list of available SLA profiles displayed. Otherwise, go to step 20.

17 Choose an SLA profile and click on the OK button. The Select SLA Profile - AntiSpoofingStaticHosts form closes, and the SLA profile name appears in the SLA Profile panel.

18 Click on the Select button in the Application Profile panel to choose an application profile for the static host, if required. The Select Application Profile - AntiSpoofingStaticHosts form opens with the list of application profiles on the NE displayed. Otherwise, go to step 20.

19 Choose an application profile and click on the OK button. The Select Application Profile - AntiSpoofingStaticHosts form closes, and the application profile name appears in the Application Profile panel.

20 Click on the Apply button if you want to create additional entries. A dialog box appears. Otherwise, go to step 23.

21 Click on the OK button.

22 Repeat steps 12 to 21 for each additional entry that you want to create.

23 Click on the OK button. A dialog box appears.

24 Click on the OK button. The Access Interface Anti-Spoofing Static Host Display (Create) form closes, and the VPLS L2 Access Interface (Edit) form refreshes with the new static host entries in a list.

25 Click on the OK button. The VPLS L2 Access Interface (Edit) form closes and a dialog box appears.

26 Click on the Yes button. The VPLS Service (Edit) form reappears.

27 Close the VPLS Service (Edit) form.

Procedure 68-37 To associate a MEP with a VPLS L2 access interface

Perform the following procedure to associate a MEP with the L2 Access interface, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you need to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface to which you want to associate a MEP and choose Properties. The VPLS L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the ETH-CFM tab.

8 Click on the Create button in the MIP Configurations panel. The MIP Configurations (Create) form opens.

9 Configure the parameters in the MIP panel:

- Primary VLAN Enable
- VLAN ID
- MAC Address



Note 1 — The Primary VLAN Enable, VLAN ID, and MAC Address parameters are configurable only when a port is assigned to the interface.

Note 2 — You cannot configure MIPs on SPB-enabled SAP and spoke SDP bindings. See "SPB in VPLS" in section 68.1 for more information about SPB.

10 Click the OK button. The MIP Configurations (Create) form closes and a dialog box is displayed.

11 Click the OK button. The new MIP Configuration is displayed in the list.

12 If you are configuring a B-L2 Access Interface then go to step 14.

13 Configure the Enable Virtual MEP Filter parameter in the Virtual MEPs panel.

14 As required, configure the Test Generation Options parameters:

- Role
- Use as Test Source
- Use as Test Target



Note — You can propagate test generation role settings to all MEPs on a SAP or service site using the Propagate to MEPs button.

15 Click on the Create button in the MEPs panel. The MEP (Create) form opens with the General tab displayed.

16 Click on the Select button in the MEP panel to choose a MEG. The Select Maintenance Entity Group form opens.

17 Click the Search button and choose an entry, then click on the OK button. The Select Maintenance Entity Group form closes and information related to your selection is displayed on the form.

18 Configure the parameters in the MEP panel:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- Description
- MAC Address
- Primary VLAN Enable
- Type
- Interface Type



Note — The Type and Interface Type parameters are automatically populated based on whether the MEP is created on a SAP, SDP binding, or Ethernet Tunnel Path Endpoint.

19 Configure the parameters in the CCM panel:

- CCM Enabled
- Priority Level for CCM
- Fault Propagation
- CCM Padding Packet Size (Bytes)
- Low-priority Defect



Note — The CCM Padding Packet Size (Bytes) parameter cannot be configured when the CCM interval parameter is set to 10 ms or 100 ms.

20 Click on the Select button in the MEG Sub-Grouping panel to choose a MEG Sub-Group, if required. The Select MEG Sub-Group form opens.

21 Click the Search button and choose an entry, then click on the OK button. The Select MEG Sub-Group form closes, and your selection is displayed on the form.

22 As required, configure the Test Generation Options parameters:

- Role
- Use as Test Source
- Use as Test Target



Note — The Test Generation Options parameters are only displayed when you set the Direction parameter to Up.

23 If the MD for the MEP has a Maintenance Domain Name Type of none and the associated MEG has a Maintenance Entity group Name Type of icc-based, then the Y.1731 Tests and AIS tabs are configurable. Click on the Y.1731 Tests tab. Otherwise, go to step 27.

24 Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

25 Click on the AIS tab.

26 Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

27 Click on the OK button. The MEP (Create) form closes.



Note 1 — If you have configured a SAP, the SAP information is filled in when you configure the MEP.

Note 2 — Once the site has been created and is operational, you can open the MEP (Edit) form and view an information field that displays the number of Continuously Running Tests currently on the MEP. This appears on the General tab of the form.

28 Enable tunnel facility MEP with the L2 Access interface, if required.

i Click on the General tab.

ii Right-click Tunnel Fault Notification and select Accept from the contextual menu.

Tunnel Fault Notification is configurable on sites where the device has ports configured in access or hybrid mode with QinQ encapsulation.

29 Click on the OK button. The VPLS L2 Access Interface (Edit) form closes and a dialog box appears.

30 Click on the Yes button. The VPLS Service (Edit) form reappears.

31 Close the VPLS Service (Edit) form.

Procedure 68-38 To assign an ANCP policy to a VPLS L2 access interface

Perform the following procedure to assign an ANCP policy to the interface, if required.

1. Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.
2. Configure the filter criteria and click on the Search button. A list of services appears.
3. Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.
4. On the navigation tree, expand the site on which you want to configure the L2 access interface.
5. Expand the L2 Access Interface object.
6. Right-click on the L2 access interface on which you want to assign an ANCP policy and choose Properties. The VPLS L2 Access Interface (Edit) form opens with the General tab displayed.
7. Click on the ANCP Static Map tab.
8. Click on the Create button. The ANCP Static Map (Create) form opens.
9. Configure the ANCP String parameter.
10. Click on the Select button to choose an ANCP Policy. The Select ANCP Policy - ANCP Static Map form opens.
11. Select an ANCP policy and click on the OK button. The Select ANCP Policy - ANCP Static Map form closes and the ANCP Static Map form reappears with the ANCP policy information displayed.
12. Click on the OK button. The ANCP Static Map form closes.
13. Click on the OK button. The VPLS L2 Access Interface (Edit) form closes and a dialog box appears.
14. Click on the Yes button. The VPLS Service (Edit) form reappears.
15. Close the VPLS Service (Edit) form.

Procedure 68-39 To configure PIM snooping on a VPLS L2 access interface

Perform the following procedure to configure PIM snooping for the interface, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface on which you want to configure PIM snooping and choose Properties. The VPLS L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the PIM Snooping tab. The General tab is displayed.

8 Configure the Max Number of Groups parameter.

9 Click on the OK button.

10 Click on the OK button. The VPLS L2 Access Interface (Edit) form closes and a dialog box appears.

11 Click on the Yes button. The VPLS Service (Edit) form reappears.

12 Close the VPLS Service (Edit) form.

Procedure 68-40 To configure MLD snooping for a VPLS L2 access interface

Perform the following procedure to configure MLD snooping for the interface, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface on which you want to configure MLD snooping and choose Properties. The VPLS L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the MLD Snooping tab. The General tab is displayed.

8 Configure the parameters:

- Import Policy
- Fast Leave
- Disable Router Alert Check
- Multicast Router Attached
- Send Queries
- General Query Interval (seconds)
- Maximum Response Interval (seconds)
- Robust count
- MLD version
- Last Member Query Interval (tenths of seconds)
- Maximum Number of Groups

The General Query Interval (seconds), Maximum Response Interval (seconds), Robust count, and MLD version parameters are configurable when the Send Queries parameter is enabled.

9 Click on the Static Mcast Group tab to configure a static multicast group, if required. Otherwise, go to step 15.

10 Click on the Create button. The Access Interface Mld Snooping Mcast Group Display (Create) form opens.

11 Configure the parameters:

- Group Address
- Source Address

12 Click on the Apply button if you want to create an additional entry. A dialog box appears. Otherwise, go to step 15.

13 Click on the OK button.

14 Repeat steps 11 to 13 to create additional entries, if required.

15 Click on the OK button. A dialog box appears.

16 Click on the OK button. The Static Mcast Group tab refreshes with the new multicast group entries.

17 Click on the OK button. The VPLS L2 Access Interface (Edit) form closes and a dialog box appears.

18 Click on the Yes button. The VPLS Service (Edit) form reappears.

19 Close the VPLS Service (Edit) form.

Procedure 68-41 To configure MVR (MLD) for a VPLS L2 access interface

Depending on the type of device that you are configuring, the MVR (MLD) tab is configurable. Use the MVR (MLD) tab to use MLD snooping on the SAP. Perform the following procedure to configure MVR for the L2 access interface, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface on which you want to configure MLD snooping and choose Properties. The VPLS L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the MVR (MLD) tab.

8 Click on the Select button in the Source MVR VPLS panel to associate an MVR VPLS with the SAP. The Select Source MVR VPLS form opens.

9 Choose a source MVR VPLS and click on the OK button. The Select Source MVR VPLS closes, and the VPLS L2 Access Interface (Create) form refreshes with the source MVR VPLS information.

10 Click on the Select button in the Proxy MVR SAP panel to choose a proxy MVR SAP to which the multicast traffic will be sent. The Select Proxy MVR SAP form opens.

11 Choose a proxy MVR SAP and click on the OK button. The Select Proxy MVR SAP form closes, and the VPLS L2 Access Interface (Edit) form refreshes with the proxy MVR SAP information.



Note — If the SAP already has an MVR proxy SAP or is the MVR proxy SAP of another SAP, the SAP cannot be an MVR proxy SAP.

12 Click on the OK button. The VPLS L2 Access Interface (Edit) form closes and a dialog box appears.

13 Click on the Yes button. The VPLS Service (Edit) form reappears.

14 Close the VPLS Service (Edit) form.

Procedure 68-42 To configure custom object attributes for AA reporting to the 5670 RAM

Perform the following procedure to configure custom object attributes for AA reporting to the 5670 RAM, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the L2 access interface.

5 Expand the L2 Access Interface object.

6 Right-click on the L2 access interface on which you want to configure custom object attributes for AA reporting to the 5670 RAM and choose Properties. The VPLS L2 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the 5670 RAM Parameters tab.

8 Click on the Reporting tab.

9 Click on the Create button. The AA Reporting (Create) form opens.

10 Configure the parameters:

- Customer Name
- Subscriber Name
- Subscriber Class
- Subscriber Type
- Total Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 1 Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 2 Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 3 Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 4 Bandwidth Upstream (Kbps)
- Downstream (Kbps)

11 Click on the OK button. The AA Reporting (Create) form closes and the reporting object is displayed in the list.

12 Click on the General tab.

13 Click on the OK button. The VPLS L2 Access Interface (Edit) form closes and a dialog box appears.

14 Click on the Yes button. The VPLS Service (Edit) form reappears.

15 Close the VPLS Service (Edit) form.

Procedure 68-43 To create a VPLS mesh SDP binding

The value of the Automatic Mesh SDP Binding Creation parameter determines the way that mesh SDP binding creation occurs in the VPLS.



Note 1 — The maximum combined number of mesh and spoke SDP bindings that you can configure on a service site depends on the NE type and release on which the site is configured. A deployment error occurs when you attempt to create an SDP binding if this limit is reached on the NE.

Note 2 — The maximum number of VPLS sites that can be automatically connected using mesh SDP bindings is 100. You can perform automatic creation of a full mesh in a VPLS in one or more passes, as required.

Alcatel-Lucent recommends that you perform automatic mesh SDP binding creation on only 50 sites at one time. Performing automatic mesh SDP binding creation on 100 sites at one time may result in a substantial delay in building the network.

Note 3 — VPLS mesh SDP bindings are not supported on the 7210 SAS-D or 7210 SAS-D.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site to which you want to add the mesh SDP binding.

5 Right-click on Mesh SDP Bindings below the site and choose Create Mesh SDP Binding. The Mesh SDP Binding (Create) form opens with the General tab displayed.

6 If automatic mesh SDP binding creation is enabled on the VPLS, a dialog box appears. The message in the dialog box discourages manual mesh SDP binding creation when automatic mesh SDP binding creation is specified for a VPLS. Perform one of the following.

a Choose not to override automatic SDP binding creation. Alcatel-Lucent recommends this action.

i Click on the No button.

ii Click on the cancel button to abort the operation and close the VPLS management form.

b Choose to override automatic SDP binding creation. Alcatel-Lucent does not recommend this action.

i Click on the Yes button. The Mesh SDP Binding (Create) form opens.

ii Consult an Alcatel-Lucent technical representative before proceeding.

7 Specify a destination NE for the mesh SDP binding:

a If the destination NE is a managed NE, choose from a list of managed NEs.

i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element - Mesh SDP Binding form opens.

ii Select a destination NE and click on the OK button. The Select Destination Network Element - Mesh SDP Binding form closes and the Mesh SDP Binding (Create) form refreshes with the tunnel termination site (the destination NE) identifier displayed.

b If the destination NE is an unmanaged NE, specify the system ID for the Tunnel Termination Site parameter.

8 Configure the parameters:

- Description
- VC Type
- VLAN VC Tag
- Ingress Label
- Egress Label

9 Perform one of the following to specify a transport tunnel for the mesh SDP binding.

a Let the 5620 SAM configure the transport tunnel automatically.

i Enable the Auto-Select Transport Tunnel parameter.

ii Configure either the Profile Name or the Tunnel Auto-Selection Transport Preference parameter.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Mesh SDP Binding form opens.

ii Select a service tunnel for the mesh SDP binding and click on the OK button. The Select Tunnel - Mesh SDP Binding form closes, and the Mesh SDP Binding (Create) form refreshes with the service tunnel identifier.

10 Configure the NE-specific parameters, as shown in Table 68-15

Table 68-15 NE-specific parameters

NE	Parameters	Dependencies
7750 SR, 7450 ESS, 7710 SR, 7950 XRS	• Egress Label • Enable Hash Label • Enable Signal Capability • Force VLAN VC Forwarding	The Force VLAN VC Forwarding parameter does not appear if you are creating a Mesh SDP binding for a B-site.

11 Click on the States tab to specify whether the mesh SDP binding is in service and configure the Administrative State parameter.

12 Perform one of the following to specify a transport tunnel for the Return SDP binding, if required.



Note — You can create a return tunnel only between sites that are in the same service. If the sites are not in the same service, the Return tab does not appear.

a If you are configuring a 7750 SR, 7450 ESS, 7710 SR, 7705 SAR, or 7950 XRS, let the 5620 SAM configure the transport tunnel automatically. If you are configuring a 7210 SAS-M or 7210 SAS-X, go to step 20.

i Click on the Return tab.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Configure either the Profile Name or the Return Tunnel Auto-Selection Transport Preference parameter.

b If you are configuring a 7750 SR, 7450 ESS, 7710 SR, 7705 SAR, or 7950 XRS, configure the transport tunnel manually. If you are configuring a 7210 SAS-M or 7210 SAS-X, go to step 20.

i Click on the Return tab.

ii Click on the Select button in the Return Tunnel panel. The Select Return Tunnel - Mesh SDP Binding form opens.

iii Select a service tunnel for the mesh SDP binding and click on the OK button. The Select Return Tunnel - Mesh SDP Binding form closes and the Mesh SDP Binding (Create) form refreshes with the service Tunnel ID, Name, and Underlying Transport displayed in the Tunnel panel.

13 If you are configuring a 7705 SAR, go to step 17.

14 Click on the QoS tab.

15 Configure the required parameters in the Forwarding Plane Redirect panel:

i Click on the Network Policy Select button to assign a policy to the Spoke SDP Binding. The Select Network Policy form opens.

ii Choose a policy from the list and click on the OK button. The Network Policy form closes.

iii Click on the Ingress Queue Group Template Policy Select button to assign a policy to the Spoke SDP Binding. The Select Ingress Queue Group Template Policy form opens.

iv Choose a policy from the list and click on the OK button. The Ingress Queue Group Template Policy form closes.

v Configure the Instance ID parameter.

16 Configure the required parameters in the Port Redirect panel:

i Click on the Network Policy Select button to assign a policy to the Spoke SDP Binding. The Select Network Policy form opens.

ii Choose a policy from the list and click on the OK button. The Network Policy form closes.

iii Click on the Egress Queue Group Template Policy Select button to assign a policy to the Spoke SDP Binding. The Select Egress Queue Group Template Policy form opens.

iv Choose a policy from the list and click on the OK button. The Egress Queue Group Template Policy form closes.

v Configure the Instance ID parameter.

17 Click on the Pseudowire OAM tab.

18 Configure the Control Word parameter.

19 Assign ingress and egress ACL filters to the mesh SDP binding, if required.

i Click on the ACL tab.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - Mesh SDP Binding form opens.

iii Select an ingress ACL filter and click on the OK button. The Select Ingress Filter - Mesh SDP Binding form closes, and the Mesh SDP Binding (Create) form refreshes with the ingress ACL filter name.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - Mesh SDP Binding form opens.

v Select an egress ACL filter and click on the OK button. The Select Egress Filter - Mesh SDP Binding form closes, and the Mesh SDP Binding (Create) form refreshes with the egress ACL filter name.

vi Click on the Select button in the IPv6 Ingress Filter panel to choose an IPv6 ingress ACL filter. The Select IPv6 Ingress Filter - Mesh SDP Binding form opens.

vii Select an IPv6 ingress ACL filter and click on the OK button. The Select IPv6 Ingress Filter - Mesh SDP Binding form closes and the Mesh SDP Binding (Create) form reappears with the IPv6 ingress ACL filter information displayed.

viii Click on the Select button in the IPv6 Egress Filter panel to choose an IPv6 egress ACL filter. The Select IPv6 Egress Filter - Mesh SDP Binding form opens.

ix Select an IPv6 egress ACL filter and click on the OK button. The Select IPv6 Egress Filter - Mesh SDP Binding form closes and the Mesh SDP Binding (Create) form reappears with the IPv6 egress ACL filter information displayed.

20 Configure anti-spoofing for the mesh SDP binding, if required.

i Click on the Anti-Spoofing tab.

ii Configure the MAC Pinning parameter.

21 Assign an accounting policy to the mesh SDP binding, if required.

i Click on the Accounting tab.

ii Configure the Collect Accounting Statistics parameter.

iii Click on the Select button to choose an accounting policy. The Select Accounting Policy - Mesh SDP Binding form opens.

iv Select an accounting policy and click on the OK button. The Select Accounting Policy - Mesh SDP Binding form closes, and the Mesh SDP Binding (Create) form refreshes with the accounting policy name.

22 Click on the OK button. The Mesh SDP Binding (Create) form closes, and a dialog box appears.

23 Click on the Yes button. The VPLS Service (Edit) form reappears.

24 Repeat steps 5 to 23 for each additional mesh SDP binding that you want to create.

25 Click on the OK button. A dialog box appears.

26 Click on the Yes button. The VPLS Service (Edit) form closes.

27 Close the Manage Services form.

28 To assign a DoS protection policy to the mesh SDP binding, perform Procedure 68-46.

29 To add or delete MFIB allowed daughter cards or configure MRP on the mesh SDP binding, perform Procedure 68-47.

30 To configure DHCP on the mesh SDP binding, perform Procedure 68-48.

31 To configure IGMP snooping on the mesh SDP binding, perform Procedure 68-49.

32 To associate a MEP to the mesh SDP binding, perform Procedure 68-50.

33 To configure MLD snooping on the mesh SDP binding, perform Procedure 68-51.

Procedure 68-44 To create a VPLS spoke SDP binding

Note 1 — The maximum combined number of mesh and spoke SDP bindings that you can configure on a service site depends on the NE type and release on which the site is configured. A deployment error occurs when you attempt to create an SDP binding if this limit is reached on the NE.

Note 2 — You cannot create a spoke SDP binding on an MVPLS site that runs MSTP. Likewise, you cannot enable MSTP for a site that has a spoke SDP binding, or on a SAP with a non-zero encapsulation value.

Note 3 — For services employing BGP AD and BGP VPLS, you should create SDP bindings manually at non-BGP AD or BGP VPLS enabled sites, or to other BGP AD or BGP VPLS sites where auto-created pseudowires are not expected to be created.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 If you are creating a redundant spoke SDP binding under an endpoint, go to step 5. Otherwise go to step 8.

Note — Redundant spoke SDP bindings under an endpoint are only valid for VPLS regular sites and B-Sites. They do not apply to I-Sites.

5 On the navigation tree, expand the site on which you want to create a redundant spoke SDP binding under an endpoint.

6 On the navigation tree, expand the endpoint on which you want to create a redundant spoke SDP binding.

7 Right-click on Spoke SDP Bindings below the endpoint and choose Create Spoke SDP Bindings. The Spoke SDP Binding (Create) form opens with the General tab displayed. Go to step 10.

8 On the navigation tree, expand the site on which you want to create a VPLS spoke SDP binding.

9 Right-click on Spoke SDP Bindings and choose Create Spoke SDP Bindings. The Spoke SDP Binding (Create) form opens with the General tab displayed.

10 Perform one of the following to specify a destination NE for the spoke SDP binding.

a If the destination NE is a managed NE, choose from a list of managed NEs.

i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element - Spoke SDP Binding form opens.

ii Select a destination NE and click on the OK button. The Select Destination Network Element - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the tunnel termination site (the destination NE) identifier.

b If the destination NE is an unmanaged NE, specify the system ID for the Tunnel Termination Site parameter.

11 Configure the parameters:

- Description
- Auto-Assign ID
- VC ID
- VC Type
- VLAN VC Tag
- Ingress Label
- Egress Label

12 Configure the NE-specific parameters, as shown in Table 68-16.

Table 68-16 NE-specific parameters

NE	Parameters	Dependencies
7750 SR, 7450 ESS, 7710 SR, 7950 XRS, 7210 SAS-M, 7210 SAS-X, 7705 SAR	• Block on Mesh SDP Failure	The Block on Mesh SDP Failure parameter does not appear if you are creating a Spoke SDP binding for a B-site or an I-site.

13 Perform one of the following to specify a transport tunnel for the spoke SDP binding.

a Let the 5620 SAM configure the transport tunnel automatically.

i Enable the Auto-Select Transport Tunnel parameter.

ii Configure either the Profile Name or the Tunnel Auto-Selection Transport Preference parameter.



Note — If you are creating a Spoke SDP binding for a B-site, the Tunnel Auto-Selection Preference must be either MPLS:LDP or MPLS:RSVP. For I-sites, you can use MPLS:LDP, MPLS:RSVP, GRE, or Any.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens.

ii Select a service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier.

c Configure an MPLS-TP transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens.

ii Select an MPLS-TP service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier. See Procedure 27-1 for more information about how to create an MPLS-TP service tunnel.

14 If you are creating the spoke SDP binding for a B-Site or an I-Site, go to step 18.

15 If you are creating the spoke SDP binding under an endpoint, go to step 17.

16 Click on the Select button in the Redundancy panel to select the desired endpoint from the drop-down menu.

17 Configure the parameters:

- Ignore Standby Signalling
- Precedence

18 Choose an SHG for the spoke SDP binding, if required.

i Click on the Select button in the Split Horizon Group panel. The Select Split Horizon Group Name - Spoke SDP Binding form opens.



Note — You must configure an SHG or residential SHG on a spoke SDP binding for an HVPLS that includes another VPLS or a VLL service.

ii Select an SHG and click on the OK button. The Select Split Horizon Group Name - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the SHG name.

19 Configure the NE-specific parameters, as shown in Table 68-17.

Table 68-17 NE-specific parameters

NE	Parameters	Dependencies
7750 SR, 7450 ESS, 7710 SR 7950 XRS 7705 SAR	• Enable Hash Label • Enable Signal Capability • Enable PW Status Signaling • MIP • Force VLAN VC Forwarding	The Force VLAN VC Forwarding parameter does not appear if you are creating a Spoke SDP binding for a B-Site or an I-Site. The Enable Hash Label and Enable PW Status Signaling parameters are not configurable if you selected an MPLS-TP tunnel in step 13.
7210 SAS-M, 7210 SAS-X	• MIP • Force VLAN VC Forwarding	The Force VLAN VC Forwarding parameter does not appear if you are creating a Spoke SDP binding for a B-Site or an I-Site. Go to step 28.

20 Select an application profile for the spoke SDP binding.

i Click on the Select button beside the Application Profile parameter. The Application Profile String: - Spoke SDP Binding form opens.

ii Configure the filter criteria. A list of application profiles appears.

iii Choose an Application Profile from the list and click on the OK button. The Application Profile String: - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form appears.



Note — The Application Profile String: - Spoke SDP Binding - VPLS service form displays only local profiles on the NE.

21 Associate an AA transit prefix policy with the spoke SDP binding, if required.



Note 1 — You can bind a transit policy to only one access interface or spoke SDP binding per NE.

Note 2 — The transit policy and the application profile must belong to the same application assurance group or partition.

i Click on the Select button in the Transit Prefix Policy panel. The Select Transit Prefix Policy form opens.

ii Select a transit prefix policy and click on the OK button.

22 Select an operational group for the spoke SDP Binding to join as a member, if required.

i Click on the Select button beside the Member Group Name parameter. The Select Operational Group - Spoke SDP Binding form opens.

ii Configure the filter criteria. A list of operational groups appears.

iii Choose an operational group from the list and click on the OK button. The Select Operational Group - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the operational group information.

23 Select an operational group for the spoke SDP Binding to monitor. Perform the following steps.

i Click on the Select button beside the Monitored Group Name parameter. The Select Operational Group - Spoke SDP Binding form opens.

ii Configure the filter criteria. A list of operational groups appears.

iii Choose an operational group from the list and click on the OK button. The Select Operational Group - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the operational group information.

24 Perform one of the following to specify a transport tunnel for the Return SDP binding, if required.



Note 1 — You can create a return tunnel only between sites that are in the same service. If the sites are not in the same service, the Return tab does not appear.

Note 2 — If you are creating a Return SDP binding for a B-site, the Return Tunnel Auto-Selection Preference must be either MPLS:LDP or MPLS:RSVP. For I-sites, you can use MPLS:LDP, MPLS:RSVP, GRE, or Any.

a Let the 5620 SAM configure the transport tunnel automatically.

i Click on the Return tab.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Configure either the Profile Name or the Return Tunnel Auto-Selection Transport Preference parameter.

b Configure the transport tunnel manually.

i Click on the Return tab.

ii Click on the Select button in the Return Tunnel panel. The Select Return Tunnel - Spoke SDP Binding form opens.

iii Select a service tunnel for the spoke SDP binding and click on the OK button. The Select Return Tunnel - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the service Tunnel ID, Name, and Underlying Transport displayed in the Tunnel panel.

25 Click on the QoS tab.

26 Configure the required parameters in the Forwarding Plane Redirect panel:

i Click on the Network Policy Select button to assign a policy to the Spoke SDP Binding. The Select Network Policy form opens.

ii Choose a policy from the list and click on the OK button. The Network Policy form closes.

iii Click on the Ingress Queue Group Template Policy Select button to assign a policy to the Spoke SDP Binding. The Select Ingress Queue Group Template Policy form opens.

iv Choose a policy from the list and click on the OK button. The Ingress Queue Group Template Policy form closes.

v Configure the Instance ID parameter.

27 Configure the required parameters in the Port Redirect panel:

i Click on the Network Policy Select button to assign a policy to the Spoke SDP Binding. The Select Network Policy form opens.

ii Choose a policy from the list and click on the OK button. The Network Policy form closes.

iii Click on the Egress Queue Group Template Policy Select button to assign a policy to the Spoke SDP Binding. The Select Egress Queue Group Template Policy form opens.

iv Choose a policy from the list and click on the OK button. The Egress Queue Group Template Policy form closes.

v Configure the Instance ID parameter.

28 Click on the States tab to specify whether the spoke SDP binding is in or out of service and configure the Administrative State parameter.

29 Click on the Pseudowire OAM tab and configure the Control Word parameter.



Note — If you are creating a spoke SDP binding using an MPLS-TP service tunnel for pseudowire static configuration, you must set the Control Word parameter to Preferred.

30 If you are configuring a 7210 SAS-M or 7210 SAS-X, go to step 33.

31 Assign ingress and egress ACL filters to the spoke SDP binding, if required.

i Click on the ACL tab.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - Spoke SDP Binding form opens.

iii Select an ingress ACL filter and click on the OK button. The Select Ingress Filter - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the ingress ACL filter name.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - Spoke SDP Binding form opens.

v Select an egress ACL filter and click on the OK button. The Select Egress Filter - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the egress ACL filter name.

vi Click on the Select button in the IPv6 Ingress Filter panel to choose an IPv6 ingress ACL filter. The Select IPv6 Ingress Filter - Spoke SDP Binding form opens.

vii Select an IPv6 ingress ACL filter and click on the OK button. The Select IPv6 Ingress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form reappears with the IPv6 ingress ACL filter information displayed.

viii Click on the Select button in the IPv6 Egress Filter panel to choose an IPv6 egress ACL filter. The Select IPv6 Egress Filter - Spoke SDP Binding form opens.

ix Select an IPv6 egress ACL filter and click on the OK button. The Select IPv6 Egress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form reappears with the IPv6 egress ACL filter information displayed.

32 If you are configuring a 7705 SAR, go to step 34.

33 Assign an accounting policy to the spoke SDP binding, if required.

i Click on the Accounting tab.

ii Configure the Collect Accounting Statistics parameter.

iii Click on the Select button to choose an accounting policy. The Select Accounting Policy - Spoke SDP Binding form opens.

iv Select an accounting policy and click on the OK button. The Select Accounting Policy - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the accounting policy name.

34 Configure anti-spoofing for the spoke SDP binding, if required.

i Click on the Anti-Spoofing tab.

ii Configure the MAC Pinning parameter.

35 If you are configuring a 7210 SAS-M or 7210 SAS-X, go to step 38.

36 Click on the MIPs tab.

37 Perform one or more of the following, if required:

a Click on the Search button to list available MIPs.

b View the current status of a specific MIP entry.

i Select a MIP from the list.

ii Click on the Properties button to display the MIP information.

c Click on the Resync button to resync the latest MIPs configured on the NE.

38 Click on the OK button. The Spoke SDP Binding (Create) form closes and a dialog box appears.

39 Click on the Yes button. The VPLS Service (Edit) form reappears.

40 Repeat steps 9 to 39 for each additional spoke SDP binding that you want to create.

41 Click on the OK button. A dialog box appears.

42 Click on the Yes button. The VPLS Service (Edit) form closes.

43 Close the Manage Services form.

44 To assign a DoS protection policy to the spoke SDP binding, perform Procedure 68-46.

45 To configure MFIB, STP, FIB, MRP, and MAC learning parameters on the spoke SDP binding, perform Procedure 68-47.

46 To configure DHCP on the spoke SDP binding, perform Procedure 68-48.

47 To configure IGMP snooping on the spoke SDP binding, perform Procedure 68-49.

48 To associate a MEP to the spoke SDP binding, perform Procedure 68-50.

49 To configure MLD snooping on the spoke SDP binding, perform Procedure 68-51.

50 To configure PIM snooping for the spoke SDP binding, perform Procedure 68-52.

51 To configure custom object attributes for AA reporting to the 5670 RAM, perform Procedure 68-53.

Procedure 68-45 To configure an MPLS-TP static pseudowire on a VPLS spoke SDP binding

Perform this procedure to create an MPLS-TP static pseudowire on the spoke SDP binding. An MPLS-TP service tunnel must be used in the SDP binding, and the Control Word parameter for pseudowire OAM must be set to Preferred. See Procedure 68-44.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens.

4 On the navigation tree, expand the site on which you want to configure the spoke SDP binding, and expand the Spoke SDP Bindings icon.

5 Click on the SDP binding on which you want to configure the MPLS-TP static pseudowire. The Spoke SDP Binding (Edit) form opens with the General tab displayed.

6 Click on the Control Channel tab.

7 Configure the parameters:

- Status
- Refresh Timer (seconds)

8 Click on the MPLS-TP PW tab.

9 Click on the Create button. The PW Path ID (Create) form opens.

10 Configure the Path AGI parameter.

11 Configure the parameters in the Source Attachment Individual Identifier panel:

- SAII Global ID
- SAII Node ID
- SAII AC ID

12 Configure the parameters in the Target Attachment Individual Identifier panel:

- TAII Global ID
- TAII Node ID
- TAII AC ID

13 Click on the OK button. The PW Path ID (Create) form closes.

14 Click on the OK button. The Spoke SDP Binding (Edit) form closes.

15 Close the VPLS Service (Edit) form.

16 Close the Manage Services form.

Procedure 68-46 To assign a DoS protection policy to a VPLS SDP binding

Perform the following procedure to assign a DoS protection policy to the SDP binding, if required.



Note — A default DoS protection policy is automatically assigned.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the VPLS mesh or spoke SDP binding, and expand Mesh SDP Bindings or Spoke SDP Bindings.

5 Right-click on the SDP binding you want to configure and choose Properties. The [Mesh|Spoke] SDP Binding (Edit) form opens with the General tab displayed.

6 Click on the Security tab.

7 Click on the Select button. The Select NE DoS Protection - [Mesh|Spoke] SDP Binding form opens.

8 Select a DoS protection policy in the list and click on the OK button. The Select NE DoS Protection - [Mesh|Spoke] SDP Binding form closes and the policy ID is displayed on the [Mesh|Spoke] SDP Binding (Edit) form.

9 Configure the MAC Monitoring parameter.

10 Configure the Ethernet CFM Monitor Flags parameter.

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The [Mesh|Spoke] SDP Binding (Edit) form closes.

13 Click on the OK button. A dialog box appears.

14 Click on the Yes button. The VPLS Service (Edit) form closes.

15 Close the Manage Services form.

Procedure 68-47 To configure MFIB, STP, FIB, MRP, and MAC learning protection parameters on a VPLS SDP binding

Perform the following procedure to configure MFIB, STP, FIB, MRP, and MAC learning protection parameters on a VPLS SDP binding.



Note 1 — The single-slot models of the 7450 ESS and 7750 SR support the addition or deletion of MFIB allowed daughter cards.

Note 2 — The MFIB Allowed Daughter Card tab does not appear if you are creating a Mesh SDP binding for a B-site.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the VPLS mesh or spoke SDP binding, and expand Mesh SDP Bindings or Spoke SDP Bindings.

5 Right-click on the mesh or spoke SDP binding you want to configure and choose Properties. The [Mesh|Spoke] SDP Binding (Edit) form opens with the General tab displayed.

6 Click on the Forwarding Control tab.

7 Perform the following if you are configuring a spoke SDP binding. Otherwise, go to step 8.

   i Depending on the device being configured, the BPDU tab is displayed.

   ii Configure the parameters:

   - L2 Protocol Termination
   - BPDU Translation

   iii Click on the STP tab.

   iv Configure the parameters:

   - Path Cost
   - Port Number
   - Priority
   - Edge Port
   - Edge Capability Detection
   - Link Type
   - Root Guard
   - Administrative State

   v Click on the FIB tab.

vi Configure the parameters:

- Aging Enabled
- Learning Enabled
- Maximum Entries
- Limit Mac Move
- Discard Unknown Source



Note — The Maximum Entries parameter does not appear if you are creating a Spoke SDP binding for a B-site.

vii Configure the NE-specific parameters, as shown in Table 68-18.

Table 68-18 NE-specific parameters

NE	Parameters	Dependencies
7750 SR, 7450 ESS, 7710 SR, 7950 XRS	• Limit Mac Move Level • Restrict Protected Source • Restrict Protected Source Action • Auto Learn MAC Protect	The Restrict Protected Source Action parameter is configurable when the Restrict Protected Source parameter is set to true.
7705 SAR	• Limit Mac Move Level	No dependencies.
7210 SAS-M, 7210 SAS-X	No NE-specific parameters.	

8 If you are configuring a mesh SDP binding, click on the FIB tab and configure the parameters. Otherwise, go to step 9.

- Restrict Protected Source
- Restrict Protected Source Action
- Auto Learn MAC Protect

9 Click on the MFIB Allowed Daughter Card tab.

10 Click on the Create button. The SDP Binding MFIB Allowed Daughter Card (Create) form opens.

11 Click on the Select button. The Select Daughter Card form opens. Select a daughter card and click OK. The Select Daughter Card form closes.

12 Click on the OK button. The SDP Binding MFIB Allowed Daughter Card (Create) form closes and a dialog box appears.

13 Click on the OK button. The Mesh SDP Binding (Edit) form displays the new allowed daughter card in the list.

14 Click on the MRP tab if you are configuring a mesh or spoke SDP binding for a B-site and configure the parameters. Otherwise, go to step 17.



Note — The MRP tab does not appear if you are creating an SDP binding for an I-site.

- MRP Join Time (tenths of a second)
- MRP Leave Time (tenths of a second)
- MRP Leave All Time (tenths of a second)
- MRP Periodic Time (tenths of a second)
- MRP Periodic Enabled

15 Click on the Select button to select an PBB MRP Policy. The Select PBB MRP Policy form opens.

16 Choose the desired policy and click on the OK button. The Select PBB MRP Policy form closes.

17 Click on the OK button. A dialog box appears.

18 Click on the Yes button. The [Mesh|Spoke] SDP Binding (Edit) form closes.

19 Click on the OK button. A dialog box appears.

20 Click on the Yes button. The VPLS Service (Edit) form closes.

21 Close the Manage Services form.

Procedure 68-48 To configure DHCP for the VPLS SDP binding

Perform the following procedure to configure DHCP for a VPLS SDP binding, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the VPLS SDP binding, and expand Mesh SDP Bindings or Spoke SDP Bindings.

5 Right-click on the SDP binding you want to configure and choose Properties. The [Mesh|Spoke] SDP Binding (Edit) form opens with the General tab displayed.

6 Click on the DHCP tab.



Note — The DHCP tab does not appear if you are configuring a mesh or spoke SDP binding for a B-site.

7 Configure the parameters:

- Description
- Snooping

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button. The [Mesh|Spoke] SDP Binding (Edit) form closes.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The VPLS Service (Edit) form closes.

12 Close the Manage Services form.

Procedure 68-49 To configure IGMP snooping for the VPLS SDP binding

Perform the following procedure to configure IGMP snooping for a VPLS SDP binding, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the VPLS SDP binding, and expand Mesh SDP Bindings or Spoke SDP Bindings.

5 Right-click on the SDP binding you want to configure and choose Properties. The [Mesh|Spoke] SDP Binding (Edit) form opens with the General tab displayed.

6 Click on the IGMP Snooping tab. The General tab is displayed.

7 Configure the parameters:

- Import Policy
- Fast Leave
- Multicast Router Attached
- Send Queries
- General Query Interval (seconds)
- Maximum Response Interval (seconds)
- Robust count
- IGMP Version
- Last Member Query Interval (tenths of seconds)
- Maximum Number of Groups
- Maximum Number of Sources per Group
- Maximum Number of Group Sources per Group

The General Query Interval (seconds), Maximum Response Interval (seconds), Robust count, and IGMP Version parameters are configurable when the Send Queries parameter is enabled.

8 Configure the NE-specific parameters, as shown in Table 68-19

Table 68-19 NE-specific parameters

NE	Parameters	Dependencies
7750 SR, 7450 ESS, 7710 SR, 7950 XRS	• Disable Router Alert Check	No dependencies.
7705 SAR	No NE-specific parameters.	
OS 9700E, OS 9800E	No NE-specific parameters.	

9 If you are configuring a 7750 SR, 7450 ESS, 7710 SR, 7950 XRS, click on the Select button in the Multicast CAC Policy panel to choose a multicast CAC policy, if required. The Select Multicast CAC Policy form opens with the list of available multicast CAC policies displayed. Otherwise, go to step 13.

10 Choose a multicast CAC policy and click on the OK button. The Select Multicast CAC Policy form closes and the multicast CAC policy information appears on the Mesh SDP Binding (Create) form.

11 Configure the parameters:

- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)
- Constraint Admin State

12 Click on the Static Mcast Group tab to configure a static multicast group, if required.

13 Click on the Create button. The Access Interface Igmp Snooping Mcast Group Display (Create) form opens.

14 Configure the parameters:

- Group Address
- Source Address

15 Click on the Apply button if you want to create additional entries. A dialog box appears. Otherwise, go to step 18.

16 Click on the OK button.

17 Repeat steps 13 to 15 to create an additional entry, if required.

18 Click on the OK button. A dialog box appears.

19 Click on the OK button. The Static Mcast Group tab refreshes with the new multicast group entries.

20 Click on the OK button. A dialog box appears.

21 Click on the Yes button. The [Mesh|Spoke] SDP Binding (Edit) form closes.

22 Click on the OK button. A dialog box appears.

23 Click on the Yes button. The VPLS Service (Edit) form closes.

24 Close the Manage Services form.

Procedure 68-50 To associate a MEP with the VPLS SDP binding

Perform the following procedure to associate a MEP with a VPLS SDP binding, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the VPLS SDP binding, and expand Mesh SDP Bindings or Spoke SDP Bindings.

5 Right-click on the SDP binding you want to configure and choose Properties. The [Mesh|Spoke] SDP Binding (Edit) form opens with the General tab displayed.

6 Click on the ETH-CFM tab.

7 Click on the Create button. The MEP (Create) form opens with the General tab displayed.

8 Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

9 Select an entry and click on the OK button. The Select Maintenance Entity Group form closes.

10 Configure the parameters:

- Auto-Assign ID
- ID
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- CCM Padding Packet Size (Bytes)



Note — The CCM Padding Packet Size (Bytes) parameter cannot be configured when the CCM interval parameter is set to 10 ms or 100 ms.

11 Configure the NE-specific parameters, as shown in Table 68-20

Table 68-20 NE-specific parameters

NE	Parameters	Dependencies
7750 SR, 7450 ESS, 7710 SR, 7950 XRS	• Direction • Fault Propagation • Fault Alarm Time (centiseconds) • Fault Reset Time (centiseconds)	No dependencies.

12 If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab. Otherwise, go to step 16.

13 Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

14 Click on the AIS tab.

15 Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

16 Click on the OK button. The MEP (Create) form closes.

17 Click on the OK button. A dialog box appears.

18 Click on the Yes button. The [Mesh|Spoke] SDP Binding (Edit) form closes.

19 Click on the OK button. A dialog box appears.

20 Click on the Yes button. The VPLS Service (Edit) form closes.

21 Close the Manage Services form.

Procedure 68-51 To configure MLD Snooping for the VPLS SDP binding

Perform the following procedure to configure MLD Snooping for a VPLS SDP binding, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the SDP binding, and expand Mesh SDP Bindings or Spoke SDP Bindings.

5 Right-click on the SDP binding you want to configure and choose Properties. The [Mesh|Spoke] SDP Binding (Edit) form opens with the General tab displayed.

6 Click on the MLD Snooping tab. The General tab is displayed.



Note — The MLD Snooping tab does not appear if you are creating a Mesh SDP binding for a B-site or I-site.

7 Configure the parameters:

- Import Policy
- Fast Leave
- Disable Router Alert Check
- Multicast Router Attached
- Send Queries
- General Query Interval (seconds)
- Maximum Response Interval (seconds)
- Robust count
- MLD version
- Last Member Query Interval (tenths of seconds)
- Maximum Number of Groups

The General Query Interval (seconds), Maximum Response Interval (seconds), Robust count, and MLD version parameters are configurable when the Send Queries parameter is enabled.

8 Click on the Static Mcast Group tab to configure a static multicast group, if required. Otherwise, go to step 14.

9 Click on the Create button. The Circuit Mld Snooping Mcast Group Display (Create) form opens.

10 Configure the parameters:

- Group Address
- Source Address

11 Click on the Apply button if you want to create an additional entry. A dialog box appears. Otherwise, go to step 14.

12 Click on the OK button.

13 Repeat steps 10 to 12 to create additional entries, if required.

14 Click on the OK button. A dialog box appears.

15 Click on the OK button. The Static Mcast Group tab refreshes with the new static multicast group entries in a list.

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The [Mesh|Spoke] SDP Binding (Edit) form closes.

18 Click on the OK button. A dialog box appears.

19 Click on the Yes button. The VPLS Service (Edit) form closes.

20 Close the Manage Services form.

Procedure 68-52 To configure PIM snooping for the VPLS SDP binding

Perform the following procedure to configure PIM snooping for a VPLS SDP binding, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the SDP binding, and expand Mesh SDP Bindings or Spoke SDP Bindings.

5 Right-click on the SDP binding you want to configure and choose Properties. The [Mesh|Spoke] SDP Binding (Edit) form opens with the General tab displayed.

6 Click on the PIM Snooping tab. The General tab is displayed.



Note — The PIM Snooping tab does not appear if you are creating a mesh or spoke SDP binding for a B-Site or I-Site.

7 Configure the Max Number of Groups parameter.

8 Click on the OK button.

9 Click on the OK button. A dialog box appears.

10 Click on the Yes button. The [Mesh|Spoke] SDP Binding (Edit) form closes.

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The VPLS Service (Edit) form closes.

13 Close the Manage Services form.

Procedure 68-53 To configure custom object attributes for AA reporting to the 5670 RAM for a spoke SDP binding

Perform the following procedure to configure custom object attributes for AA reporting to the 5670 RAM for a spoke SDP binding.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the site on which you want to configure the spoke SDP binding, and expand Spoke SDP Bindings.

5 Right-click on the SDP binding you want to configure and choose Properties. The Spoke SDP Binding (Edit) form opens with the General tab displayed.

6 Click on the 5670 RAM Parameters tab.

7 Click on the Reporting tab.

8 Click on the Create button. The AA Reporting (Create) form opens.

9 Configure the parameters:

- Customer Name
- Subscriber Name
- Subscriber Class
- Subscriber Type
- Total Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 1 Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 2 Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 3 Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 4 Bandwidth Upstream (Kbps)
- Downstream (Kbps)

10 Click on the OK button. The AA Reporting (Create) form closes and the reporting object is displayed in the list.

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The Spoke SDP Binding (Edit) form closes.

13 Click on the OK button. A dialog box appears.

14 Click on the Yes button. The VPLS Service (Edit) form closes.

15 Close the Manage Services form.

Procedure 68-54 To configure a site for BGP AD or BGP VPLS

This procedure provides the steps required to enable BGP Auto Discovery or configure BGP VPLS on a VPLS site.

- BGP AD enables a VPLS PE router to discover other PE routers that are part of the same VPLS domain. T-LDP based label signaling is used for the pseudowire.
- BGP VPLS provides the mechanism for service member auto-discovery based on Route Target. MP-BGP based label signaling is used for the pseudowire.



Note 1 — BGP AD and BGP VPLS implementations only apply to regular VPLS sites and B-Sites, but not to I-Sites. For BGP VPLS, the B-Site cannot be used as a backbone for an I-Site or Epipe.

Note 2 — For the 7210 SAS-M and 7210 SAS-X, BGP AD only is supported on VPLS service sites (not on MPVLS or B-sites).

1 Prior to configuring a site for BGP AD or BGP VPLS, you must complete the following actions:

i Create a routing policy to define the required community members. See Procedure 22-15. This defines the VSI Import/Export Routing Targets.

ii Enable BGP on the routing instance of each NE in the VPLS or BGP VPLS. See Procedure 23-1 for more information.

iii Configure global-level BGP on each NE in the VPLS or BGP VPLS. See Procedure 23-2 for more information. The following items are required for BGP AD implementation.

- You must enable the L2 VPN parameter in the Family panel on one or more of the following:
  - the VPN tab of the BGP Site form
  - the VPN tab of the BGP Peer Group form, which contains the peers that are involved in the BGP signaling
  - the VPN tab of the BGP peer form, which participates in BGP signaling
- Create a peer group under BGP. This peer group is used to collectively define the peers involved in the VPLS.
- Create the required peers under the peer group. These peers are the NEs involved in the VPLS.

iv Create a PW template policy. See chapter 73 for information about PW template policies.

v Distribute the PW template policy to each NE that is or will be a component of the VPLS or BGP VPLS.

vi Ensure that the BGP AD Administrative Status parameter is set to Up and that the VPLS ID parameter is configured.

2 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

3 Configure the filter criteria and click on the Search button. A list of services appears.

4 Select the required VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

5 Perform one of the following:

a On the navigation tree, right-click on the required site and choose Properties. The VPLS Site (Edit) form opens with the General tab displayed.

b Create a new site. Perform steps 4 to 8 in Procedure 68-7.

6 Click on the BGP tab. The General tab is displayed.

7 Enable the Enable BGP parameter. The BGP section is displayed.

8 Configure the Route Distinguisher parameter.

9 Click on the Configuration button to configure the Route Targets and the PW template policies. The BGP Configuration form opens, with the VSI Import Policies tab displayed.

10 Select up to five import policies, as required. Alternatively, you can enter the policy names manually in the provided fields.

11 Perform one of the following:

a Enter the Import Route Target name manually in the provided field. The format be “target:x:y”.

b Click on the Import Route Target Select button. The Select...-BGP Info form opens. Click on the Search button to display the available import route targets. The community members you defined when creating a routing policy in step 1 appear in the list. Select the required target and click OK. The Select...-BGP Info form closes.

12 Click on the VSI Export Policies tab and select up to five export policies, as required. Alternatively, you can enter the policy names manually in the provided fields.

13 Perform one of the following:

a Enter the Export Route Target name manually in the provided field. The format must be “target:x:y”.

b Click on the Export Route Target Select button. The Select...-BGP Info form opens. Click on the Search button to display the available export route targets. The community members you defined when creating a routing policy in step 1 appear in the list. Select the required target and click OK. The Select...-BGP Info form closes.

14 Click on the PW Template Binding tab.

15 Perform one of the following:

a To use an existing PW Template Binding, go to step 16.

b To add a new PW Template Binding, go to step 17.

16 To use an existing PW Template Binding:

i Click on the Search button. A list of applicable PW Template Bindings is displayed.

ii Select the required entry or entries from the list.

iii Go to step 18.

17 To create a new PW Template Binding:

i Click on the Create button. The PW Template Binding (Create) form opens with the General tab displayed.

ii Enter a Split Horizon Group name, if required.

iii Click on the Select button. The Select PW Template form is displayed.

iv Click on the Search button. A list of applicable PW Templates is displayed.

v Select the PW Template you created in step 1.

vi Click on the OK button to accept the selection. The Select PW Template form close and the Policy ID field is populated by your choice.

vii Click on the Select button beside the Member Group Name parameter. The Select Operational Group - PW Template Binding form opens.

viii Configure the filter criteria. A list of operational groups appears.

ix Choose an operational group from the list and click on the OK button. The Select Operational Group - PW Template Binding form closes and the PW Template Binding (Create) form refreshes with the operational group information.

x Click on the PW Templates Binding Route Target tab and click on the Create button. The PW Template Binding Route Target (Create) form is displayed.



Note — This Import Route Target is used by the NE to decide which PW Template to use to create SDP bindings. If a far-end neighbor has a matching export target (that is, to the PW Template Import Target being defined here), then this PW Template is selected by the NE to create the pseudowire that is used to link both sites of the VPLS. If nothing is entered, and multiple PW Templates are defined, the first one found by the NE is used (most likely the one with the lowest PW Template Policy ID).

Enter the required Import Route Target in the field and click OK. The PW Template Binding Route Target (Create) form closes and the entered Import Route Target is displayed in the table on the PW Template Binding Route Target tab.

xi Click on the OK button to accept the selection. The PW Template Binding (Create) form closes and the new PW Template Binding is displayed in the table on the PW Template Binding tab.

xii Repeat steps i to xi to create additional PW Template Bindings, as required.

xiii Select the required entry or entries from the list.

18 Click on the OK button to apply the configuration changes you have made. The BGP Configuration form closes.

19 If you are configuring a BGP VPLS, go to step 20. Otherwise go to step 23.

20 Enable the Enable BGP VPLS parameter. The BGP VPLS section is displayed.

21 Configure the parameters:

- VE Name
- Max VE ID
- VE ID
- Administrative State

22 Select an operational group for the BGP site to monitor. Perform the following steps.



Note — This step does not apply to the 7210 SAS-M or 7210 SAS-X.

i Click on the Select button beside the Monitored Group Name parameter. The Select Operational Group - BGP Multi-homing VPLS site form opens.

ii Configure the filter criteria. A list of operational groups appears.

iii Choose an operational group from the list and click on the OK button. The Select Operational Group - BGP Multi-homing VPLS site form closes and the BGP Multi-homing VPLS site (Create) form refreshes with the operational group information.

23 If you are configuring BGP AD, go to step 24. Otherwise go to step 27.

24 Enable the Enable BGP AD parameter. The BGP AD section is displayed.

25 Configure the parameters:

- VPLS ID
- Formatted VSI ID Prefix
- Administrative State



Note 1 — The Global Service VPLS ID is set to the value defined at the service level.

Note 2 — If VPLS ID is defined at the service level, then the 5620 SAM ensures that each site has the same VPLS ID. If a site has a different VPLS ID, an alarm is raised and the ID mismatch is indicated in the Status panel of the VPLS site properties form.

The same VPLS ID value is propagated to each site in a VPLS. If you change the VPLS ID of a site without using the 5620 SAM, the 5620 SAM displays a warning form.

26 Click on the OK button. The VPLS Site (Edit) form closes.

27 Click on the OK button. A dialog box appears.

28 Close the VPLS Service (Edit) form.

Procedure 68-55 To configure a site for BGP VPLS Multi-homing

This procedure provides the steps required to configure a site for BGP VPLS Multi-homing. BGP VPLS Multi-homing provides redundancy support through the configuration of a number of multi-homed sites, rather than through the use of MC-LAG or MC-Ring as access mechanisms. Dual-homing between a CE device and a pair of VPLS PE devices (potentially in different autonomous systems) is an example of such a configuration.



Note 1 — Only regular VPLS sites and B-Sites can be configured for BGP VPLS Multi-homing. However, the B-Sites cannot be used as a backbone for an I-Site or Epipe.

Note 2 — I-VPLS and MVPLS services cannot be configured for this application.

Note 3 — An RD or RT configured under the BGP of a VPLS site cannot be removed as long as there is a multi-homing site ID configured whose administration state is up.

Note 4 — You can see a list of all current BGP VPLS Multi-homing sites in a multi-homing VPLS service by viewing the BGP Multi-homing Sites tab on the service configuration form.

1 Prior to configuring a site for BGP VPLS Multi-homing, you must complete the following actions:

i Create a routing policy to define the required community members. See Procedure 22-15 for more information. This defines the VSI Import/Export Routing Targets.

ii Enable BGP on the routing instance of each NE in the VPLS or BGP VPLS. See Procedure 23-1 for more information.

iii Configure global-level BGP on each NE in the VPLS or BGP VPLS. See Procedure 23-2 for more information. The following items are required:

- Enable the L2 VPN parameter on one or more of the following:
  - the VPN tab of the BGP site form
  - the VPN tab of the BGP Peer Group form, which contains the peers that are involved in the BGP multi-homing
  - the VPN tab of the BGP peer form, which participates in BGP signaling
- Create a peer group under BGP. This peer group is used to collectively define the peers involved in the VPLS.
- Create the required peers under the peer group. These peers are the NEs involved in the VPLS.



Note — For optimal processing while a BGP multi-homing site is activated or de-activated, or the system is rebooted, you should also:

- Enable the L2 VPN parameter in the Rapid Update Address Family panel on the BGP site VPN tab.
- Enable the Enable Rapid Withdrawal parameter on the BGP site Behavior tab.

iv Create a PW template. See chapter 73 for information about PW templates.

v Distribute the PW Template to each NE that is or will be a component of the VPLS or BGP VPLS.

vi Create SDPs for the BGP VPLS Multi-homing site(s), if manually-provisioned service tunnels are required. Refer to Procedure 27-1.

2 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

3 Configure the filter criteria and click on the Search button. A list of services appears.

4 Select the required VPLS or HVPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

5 Perform one of the following:

i On the navigation tree, right-click on the required site and choose Properties. The VPLS Site (Edit) form opens with the General tab displayed.

ii Create a new site. Perform steps 4 to 8 in Procedure 68-7.

6 Click on the BGP tab. The General tab is displayed.

7 Enable the Enable BGP parameter. The BGP section is displayed.

8 Configure the Route Distinguisher parameter.

9 Click on the Configuration button to configure the Route Targets and the PW Templates. The BGP Configuration form opens, with the VSI Import Policies tab displayed.

10 Select up to five import policies, as required. Alternatively, you can enter the policy names manually in the provided fields.

11 Perform one of the following:

a Enter the Import Route Target name manually in the provided field. The format must be “target:x:y”.

b Click on the Import Route Target Select button. The Select... -BGP Configuration form opens. Click on the Search button to display the available import route targets. The community members you defined when creating a routing policy in step 1 appear in the list. Select the required target and click OK. The Select... -BGP Configuration form closes.

12 Click on the VSI Export Policies tab and select up to five export policies, as required. Alternatively, you can enter the policy names manually in the provided fields.

13 Perform one of the following:

a Enter the Export Route Target name manually in the provided field. The format must be “target:x:y”.

b Click on the Export Route Target Select button. The Select... -BGP Configuration form opens. Click on the Search button to display the available export route targets. The community members you defined when creating a routing policy in step 1 appear in the list. Select the required target and click OK. The Select... -BGP Configuration form closes.

14 Click on the PW Template Binding tab.

15 Perform one of the following:

a To use an existing PW Template Binding, go to step 16.

b To create a new PW Template Binding, go to step 17.

16 To use an existing PW Template Binding:

i Click on the Search button. A list of applicable PW Template Bindings is displayed.

ii Select the required entry or entries from the list.

iii Go to step 18.

17 To create a new PW Template Binding:

i Click on the Create button. The PW Template Binding (Create) form opens with the General tab displayed.

ii Enter a Split Horizon Group name, if required.

iii Click on the Select button. The Select PW Template form is displayed.

iv Click on the Search button. A list of applicable PW Templates is displayed.

v Select the PW Template you created in step 1.

vi Click on the OK button to accept the selection. The Select PW Template form close and the Policy ID field is populated by your choice.

vii Click on the PW Templates Binding Route Target tab and click on the Create button. The PW Template Binding Route Target (Create) form is displayed.



Note — This Import Route Target is used by the NE to decide which PW Template to use to create SDP bindings. If a far-end neighbor has a matching export target (that is, to the PW Template Import Target being defined here), then this PW Template is selected by the NE to create the pseudowire that is used to link both sites of the VPLS. If nothing is entered, and multiple PW Templates are defined, the first one found by the NE is used (most likely the one with the lowest PW Template Policy ID).

Enter the required Import Route Target in the field and click OK. The PW Template Binding Route Target (Create) form closes and the entered Import Route Target is displayed in the table on the PW Template Binding Route Target tab.

viii Click on the OK button to accept the selection. The PW Template Binding (Create) form closes and the new PW Template Binding is displayed in the table on the PW Template Binding tab.

ix Repeat steps i to viii to create additional PW Template Bindings, as required.

x Select the required entry or entries from the list.

18 Click on the OK button to apply the configuration changes you have made. The BGP Configuration form closes.

19 Click on the Multi-homing tab.

20 Click on the Create button. The BGP Multi-homing Site (Create) form opens.

21 Configure the parameters:

- Multi-homing Site Name
- Multi-homing ID
- Enable Multi-homing to

22 Click on the Select button to specify a SAP, Spoke SDP, Split Horizon Group, or Mesh SDP Binding, based on the option you selected for the Enable Multi-homing to parameter. The appropriate selection form opens to allow you to search for the required object.

23 Select the required object and click OK. The selection form closes and the BGP Multi-homing Site (Create) form is refreshed to display the selected object.

24 Configure the parameters:

- Failed Threshold
- Use Node Level Boot Timer
- Boot Timer (seconds)
- Use Node Level Site Activation Timer
- Activation Timer (seconds)
- Administrative State

If you enable either the Use Node Level Boot Timer and/or Use Node Level Site Activation Timer parameters, then the associated Boot Timer (seconds) and/or Activation Timer (seconds) parameters will not be configurable. These parameter values will be inherited from the network element configuration.

The Boot Timer (seconds) and Activation Timer (seconds) parameters can be configured for an NE on the BGP Multi-homing tab under the Redundancy tab in the Network Element (Edit) form. See Procedure 13-2 for more information on changing device properties.

25 Click on the Select button to specify a Monitored Group Name. The Select Monitored Group Name form is displayed.

26 Click on the Search button to display a list of eligible Monitored Group Names.

27 Select the required Monitored Group Name and click OK. The Select Monitored Group Name form closes and the BGP Multi-homing Site (Create) form is refreshed to display the selected Monitored Group Name.

28 Click on the Apply button. A dialog box appears.

29 Click on the OK button. The BGP Multi-homing VPLS Site (Create) form refreshes.

30 Check the following indicators:

- Operational State: indicates the operational status of the multi-homing site.
- Designated Forwarder: indicates whether this site has been declared as designated forwarder, depending on the result of the BGP election.

31 Click on the OK button. The BGP Multi-homing VPLS Site (Create) form closes.

32 Click on the OK button. The VPLS Site (Edit) form closes.

33 Close the VPLS Service (Edit) form.

Procedure 68-56 To re-evaluate the PW Templates associated with a BGP AD or BGP VPLS

Use this procedure to re-evaluate changes made to the Route Targets associated with the PW Template bindings of an existing site with BGP configuration. This procedure can only be performed on an existing VPLS that has been configured with BGP AD or BGP VPLS. The procedure allows you to make configuration changes and propagate them to the service without having to shutdown and then turn up a site.

1 Choose Manage→Service→Services from the 5620 SAM main menu.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Select the required VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, right-click on the required site and choose Properties. The VPLS Site (Edit) form opens with the General tab displayed.

5 Click on the BGP tab.

6 Click on the Configuration button to open the BGP Configuration form.

7 Make any required changes to the Route Targets or PW Template bindings. See Procedures 68-54 or 68-55 as required, for detailed instructions on configuring these items.

8 Click on the PW Template Binding tab and click on the Apply button to apply the changes you have made.

9 Perform one of the following:

a If you need to update the PW Templates under other sites for this service, repeat steps 4 to 8 as required, then go to step 13.

b If you do not need to update the PW Templates under other sites for this service go to step 10.

10 Click on the Re-evaluate PW Template button to run an evaluation of the PW Template bindings. A pop-up window appears indicating if the re-evaluation was successful. If it was not, the reason for the failure is displayed.

If you make any subsequent modifications, you can re-evaluate the template again.

11 Click on the OK button. The BGP Configuration form closes.

12 Click on the OK button to close the VPLS Service (Edit) form. The procedure is complete.

13 Return to the VPLS Service (Edit) form.

14 Click on the Re-evaluate PW Template button. The Add form opens to allow you to select one of the PW Templates you modified.

15 Click on the Search button to display a list of PW Templates and select the required one.

16 Click on the OK button to run an evaluation of the selected PW Template. A pop-up window appears indicating if the re-evaluation was successful. If it was not, the reason for the failure is displayed.

17 Repeat steps 14 to 16 for any other sites that you want to re-evaluate a PW Template for.

18 Click on the OK button to close the VPLS Service (Edit) form.

Procedure 68-57 To assign tunnel administrative groups to a BGP or BGP AD VPLS

Perform this procedure to assign tunnel administrative groups to a BGP or BGP AD VPLS. The tunnel administrative groups are applicable only when the VPLS is configured as a PBB tunnel. The VPLS must be configured to include B-sites and Multi-Segment Tunnel Selection must be enabled in the system preferences. See chapter 79 for more information about tunnel administrative groups.

1 Choose Manage→Service→Services from the 5620 SAM main menu.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Select the required BGP or BGP AD VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 Click on the Tunnel Admin Groups tab.

5 Select the tunnel administrative groups in the Unassigned list that you want to assign to the tunnel and click the right arrow to move them into the Assigned list.

6 Click on the OK button to close the VPLS Service (Edit) form.

7 Close the Manage Services form.

Procedure 68-58 To create an HVPLS

Perform this procedure to create an HVPLS. An HVPLS consists of a VPLS in which one or more sites connect to other sites in the same VPLS, different VPLS, or to VLL services.



Note — One VPLS site in an HVPLS must be configured with an SHG. See "Split horizon groups" in this chapter for more information.

1 Add a VPLS to the HVPLS.

a Create a new VPLS.

i Perform Procedure 68-1.



Caution — If you are creating an HVPLS that includes two sites in the same VPLS connected by spoke SDPs, do not create mesh SDP bindings between the sites. Mesh SDP binding functionality is available in the spoke SDP bindings between the sites.

ii Go to step 2.

b Use an existing VPLS. Go to step 3.

2 Create another service for inclusion in the HVPLS, if required.

a Create a VPLS.

i Perform Procedure 68-1.

ii Go to step 3.

b Create a VLL.

i Perform the appropriate VLL creation procedure in chapter 67.

ii Go to step 3.

3 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens with the General tab displayed.

4 Configure the filter criteria. A list of services appears.

5 Choose a VPLS that you want to include in the HVPLS and click on the OK button. The VPLS Service (Edit) form opens.

6 Right-click on Spoke SDP Bindings below the site and choose Create Spoke SDP Bindings. The Spoke SDP Binding (Create) form opens with the General tab displayed.

7 Perform steps 10 to 51 Procedure 68-44. Choose the destination NE for the site that you want to include in the HVPLS as the Tunnel Termination Site.

8 Perform Procedure 68-7 to add sites to the HVPLS.

Procedure 68-59 To create an MVPLS

An MVPLS runs RSTP or MSTP to manage traffic blocking on the associated VPLS. Perform this procedure to create an MVPLS to run MSTP, or to run RSTP and manage traffic on the associated VPLS SAPs or redundant spoke SDPs. The procedure also applies to the I-Sites and B-Sites used in PBB.

1 Choose Create→Service→MVPLS from the 5620 SAM main menu. The MVPLS service (Edit) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the MVPLS. The Select Customer - MVPLS form opens.

3 Select a customer for the MVPLS and click on the OK button. The Select Customer - MVPLS form closes, and the MVPLS service (Edit) form refreshes with the customer name.

4 Configure the parameters:

- Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Auto-Assign ID
- SVC Mgr Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Service Name
- Description
- Service Tier
- Service Priority
- Administrative State
- Default Mesh VC ID
  This parameter is configurable when the Inherit Service ID Value parameter is disabled.
- Inherit Service ID Value
- Per Service Hashing for LAG Enabled

5 Configure the OLC state:

i Click on the Apply button.

ii Configure the parameters:

- Current OLC State
- Revert OLC State

6 To configure service tunnel required bandwidth for the service, perform the following steps.



Note — In order to configure service tunnel required bandwidth, you must enable multi-segment tunnel selection and service bandwidth management at the system level.

i Click on the Bandwidth tab.

ii Configure the Bandwidth Method parameter.

iii If the Bandwidth Method parameter is set to Manual or Calculate, configure LSP Path Booking parameter.

iv If the Bandwidth Method parameter is set to Manual, enter a required bandwidth value for each CoS (see CoS 0 Bandwidth - CoS 7 Bandwidth).

7 On the navigation tree, right-click on Sites under MVPLS and choose one of the following, as required:

- Create MVPLS B-Site
- Create MVPLS I-Site
- Create MVPLS Site

The Select Network Elements - MVPLS form opens with a list of available sites.

8 Select a site and click on the OK button. Depending on your selection in step 7, the MVPLS B-Site (Create), MVPLS I-Site (Create), or MVPLS Site (Create) form opens with the General tab displayed.

9 Perform one of the following:

a Create an RSTP site for the MVPLS.

i For regular VPLS sites, perform steps 5 to 7 of Procedure 68-7. Specify RSTP as the value for the STP Mode parameter in step 7 of Procedure 68-8. Go to step iv when completed.

ii For B-Sites, perform steps 6 to 20 of Procedure 68-60. Specify RSTP as the value for the STP Mode parameter in step 9iv. Go to step iv when completed.

iii For I-Sites, perform steps 10 to 22 of Procedure 68-65. Specify RSTP as the value for the STP Mode parameter in step 14 iv. Go to step iv when completed.

iv Repeat step i, ii, or iii, as required, for each site that you want to create in the MVPLS.

b Create an MSTP site for the MVPLS.



Note — MSTP is configurable only on the 7210 SAS-D, 7210 SAS-E, 7450 ESS, 7750 SR, and 7950 XRS.

i For regular VPLS sites, perform steps 5 to 7 of Procedure 68-7. Specify MSTP as the value for the STP Mode parameter in step 7 of Procedure 68-8. Go to step iv when completed.

ii For B-Sites, perform steps 6 to 20 of Procedure 68-60. Specify MSTP as the value for the STP Mode parameter in step 9iv. Go to step iv when completed.

iii For I-Sites, perform steps 10 to 22 of Procedure 68-65. Specify MSTP as the value for the STP Mode parameter in step 14iv. Go to step iv when completed.

iv Repeat step i, ii, or iii, as required, for each site that you want to create in the MVPLS.

10 Click on the OK button. The MVPLS service (Edit) form reappears.

11 If the MVPLS site is to manage traffic on associated VPLS SAPs, create a SAP for the MVPLS with a defined redundant VLAN range.



Note — If an MVPLS site has SAPs that manage traffic on the associated VPLS SAPs, you must define a redundant VLAN range during SAP creation in the MVPLS.

i For regular VPLS sites, perform steps 5 to 33 of Procedure 68-24. Ensure that you perform Procedure 68-31to specify a redundant VLAN range. Go to step iv when completed.

ii For B-Sites, perform steps 5 to 27 of Procedure 68-66. Ensure that you perform step 22 to specify a redundant VLAN range. Go to step iv when completed.

iii For I-Sites, perform steps 5 to 30 of Procedure 68-70. Ensure that you perform step 24 to specify a redundant VLAN range. Go to step iv when completed.

iv Click on the OK button. The MVPLS service (Edit) form reappears.

12 Click on the OK button. The MVPLS service (Edit) form closes.

Procedure 68-60 To create a B-site for VPLS or MVPLS

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Select the required VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, right-click on the Sites icon and choose Create VPLS B-Site from the contextual menu. The Select Network Elements - VPLS form opens with a list of available sites.

5 Select a site and click on the OK button. The B-Site (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Name
- Description
- MTU
- Default Mesh VC ID
- Administrative State
- Monitor Access Interface Operational State
- Per Service Hashing for LAG Enabled

7 Click on the Backbone tab. The General tab is displayed.

8 Configure the backbone parameters:

- Source MAC Address
- Use SAP Backbone MAC Address
- Administrative State
- MAC Notification Interval (seconds)
- MAC Notification Count



Note 1 — The Source MAC Address should not be duplicated for other B-sites within the same B-VPLS.

Note 2 — The Source MAC Address parameter is the only applicable parameter when configuring PBB on a 7210 SAS-M or a 7210 SAS-X.

Note 3 — The Use SAP Backbone MAC Address parameter is configurable only on the 7750 SR, 7750 SR-c12, 7750 SR-12E, 7450 ESS, or 7950 XRS. The NE must also be configured with an IOM 3 MDA or an XMA.

9 Configure MFIB, STP, FIB, and MRP parameters for the B-site, if required.

i Click on the Forwarding Control tab. The MFib tab is displayed.

ii Configure the parameters:

- Table size (entries)
- High Watermark (%)
- Low Watermark (%)

iii Click on the STP tab to configure STP parameters for the B-site, if required. Otherwise, go to step v.

iv Configure the bridge-level STP parameters for the B-site.

Alcatel-Lucent STP in a VPLS interoperates with customer STP implementations as a mechanism for loop detection and prevention. The bridge-level parameters balance the STP resiliency and speed of convergence. Modifying the bridge-level parameters must be done within the constraints of the following formulas:

- 2 × (Bridge Forward Delay – 1.0 s) >= Bridge Max Age
- Bridge Max Age >= 2 × (Bridge Hello Time + 1.0 s)



Note 1 — If you are configuring an MVPLS B-site, set the STP Mode parameter to RSTP or MSTP, depending on the MVPLS type. The MSTP option is available only if you are creating an MVPLS. See Procedure 68-59 for more information about creating an MVPLS.

Note 2 — MSTP is configurable only on the 7450 ESS, 7710 SR, 7750 SR, and 7950 XRS.

- Bridge Forward Delay (seconds)
- Bridge Hello Time (seconds)
- Bridge Max Age (seconds)
- Priority
- STP Mode
- Maximum BPDUs (PDUs/Hello Interval)
- Administrative State

v Click on the FIB tab to configure FIB parameters for the B-site, if required. Otherwise, go to step 12.

vi Configure the parameters:

- High Watermark (%)
- Low Watermark (%)
- Local Age Time (seconds)
- Remote Age Time (seconds)
- Size (entries)
- Aging Enabled
- Learning Enabled
- Discard Unknown Destinations
- MAC Flush on fail
- Propagate MAC Flush

vii Depending on the type of device being configured, the Mac Move panel appears. Configure the MAC move parameters, if required:

- Move Frequency
- Retry Timeout
- Number of Retries
- Administrative State
- Primary Ports Cumulative Factor
- Secondary Ports Cumulative Factor

viii If you are configuring an MVPLS B-site that requires MSTP, click on the MSTP tab. Otherwise, go to step 12.



Note — MSTP is configurable only on the 7450 ESS, 7710 SR, 7750 SR, and 7950 XRS.

ix Configure the parameters:

- Region Name
- Region Revision
- Bridge Max Hops

x Click on the MST Instances tab.

xi Click on the Create button. The MST Instance (Create) form opens with the General tab displayed.

xii Configure the parameters:

- Instance Index
- Priority

xiii Click on the VLAN Ranges tab. Click on the Create button. The MST Instance Managed VLAN range (Create) form opens.

xiv Configure the parameters:

- Min. VLAN Tag
- Max. VLAN Tag

xv Click on the OK button. The MST Instance Managed VLAN Range (Create) form closes, and a dialog box appears.

xvi Click on the OK button. The MST Instance (Create) form refreshes with the new managed VLAN range.

xvii Click on the OK button. The MST Instance (Create) form closes and a dialog box appears.

xviii Click on the OK button. The MVPLS Site (Create) form refreshes with the new MST instance.

xix Click on the MRP tab.

xx Configure the parameters:

- MRP Admin Status
- MRP Max Attributes
- MRP Flood Time (seconds)
- MRP Attribute-Table-Low-Watermark
- MRP Attribute-Table-High-Watermark
- MMRP Endstation Only



Note — You can view information regarding MMRP Entries for the access interface and/or SDP Binding by clicking on the MMRP Entries tab.

10 To configure service tunnel required bandwidth for the site, perform the following steps.



Note — In order to configure service tunnel required bandwidth, you must enable multi-segment tunnel selection and service bandwidth management at the system level.

i Click on the Bandwidth tab.

ii Enable the Override Service Configuration parameter.

iii Configure the Bandwidth Method parameter.

iv If the Bandwidth Method parameter is set to Manual, enter a required bandwidth value for each CoS (see CoS 0 Bandwidth - CoS 7 Bandwidth).

11 Configure a Provider Tunnel for the site, if required.

When you configure an inclusive Provider Tunnel, multicast and broadcast Ethernet frames are always forwarded over a P2MP LSP, defined as the Inclusive Provider Multicast Service Interface (I-PMSI). When a Provider Tunnel is not configured, these frames are replicated at the ingress PE and a copy of each frame is forwarded over the P2P PW to each destination PE participating in the VPLS instance. Provider Tunnels can be configured on VPLS and B-VPLS sites.



Note — Provider tunnels are supported on the 7750 SR-7, 7750 SR-12, 7750 SR-c4, 7750 SR-c12, 7750 SR-12E, and 7450 ESS NEs in all chassis modes, as well as on the 7540 ESS, provided all network IP interfaces are on IOM3/IMM ports (chassis mode D).

i Click on the Provider Tunnel tab.

ii Enable the Enable Provider Tunnel parameter.

iii Configure the parameters:

- Administrative State
- Data Delay Interval (seconds)
- Root And Leaf
- Type
- LSP Template

The Administrative State parameter is only configurable when the Enable BGP AD parameter has been enabled for the site.

The LSP Template parameter is only configurable when the Type parameter is set to RSVP.

12 Create an endpoint for redundancy (dual homing) on the B-site, if required.

i Click on the Endpoints tab.

ii Click on the Create button. The Endpoint (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Name
- Description
- Revert Time (seconds)
- Suppress Standby Signalling
- Ignore Standby Signalling
- MAC Pinning

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Endpoint (Create) form closes and the B-Site (Create) form reappears with the new endpoint displayed in the list.

13 If you are configuring an MVPLS B-site, go to step 17.

14 Configure an SHG on the site, if required.



Note — You must configure an SHG or RSHG if you plan to create a spoke circuit from this VPLS B-site to a VLL or to another VPLS.

i Click on the Split Horizon Groups tab.

ii Click on the Create button. The Site, New Split Horizon Group (Create) form opens.

iii Configure the parameters:

- Name
- Description

iv Click on the OK button. The Site, New Split Horizon Group (Create) form closes.



Note — You can view information about the I-Sites and Epipe sites associated with the B-Site by clicking on the Associated Sites tab.

15 To create a B-L2 access interface for the site, perform steps 5 to 29 of Procedure 68-66.

16 To create a mesh SDP binding for the site, perform steps 5 to 24 of Procedure 68-43.

17 To create a redundant spoke SDP binding under an endpoint, perform steps 4 to 40 of Procedure 68-44.

18 To create a spoke SDP binding for the site, perform steps 7 to 40 of Procedure 68-44.



Note 1 — You cannot create a spoke SDP binding on an MVPLS site that runs MSTP, or enable MSTP on a site that has a spoke SDP binding.

Note 2 — You cannot enable MSTP on a SAP that has a non-zero encapsulation value.

19 Create a virtual MEP on the site, if required. For more information about virtual MEPs, see section 78.1.

i Click on the ETH-CFM tab.

ii Configure the Tunnel Fault Notification parameter.

iii Click on the Create button in the Virtual MEP panel. The MEP (Create) form opens.

iv Click on the Select button. The Select Maintenance Entity Group form opens.

v Choose a MEG from the list.

vi Click on the OK button. The Select Maintenance Entity Group form closes, and the MEG information is displayed on the MEP (Create) form.

vii Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- Description
- MAC Address
- CCM Enabled
- Priority Level for CCM
- Fault Propagation
- CCM Padding Packet Size (Bytes)
- Low-priority Defect



Note — The CCM Padding Packet Size (Bytes) parameter cannot be configured when the CCM interval parameter is set to 10 ms or 100 ms.

viii As required, configure the Test Generation Options parameters:

- Role
- Use as Test Source
- Use as Test Target



Note — The Role, Use as Test Source, and Use as Test Target parameters are configurable only when you set the Direction parameter to Up.

ix Click on the OK button. The MEP (Create) form closes, and the virtual MEP is created on the B-VPLS site.



Note — After the site is created and is operational, you can open the MEP (Edit) form and view an information field on the General tab that displays the number of Continuously Running Tests currently on the MEP.

20 Click on the OK button. The B-Site (Create) form closes, and a dialog box appears.

21 Click on the OK button. The VPLS Service (Create) form displays the new site on the navigation tree under VPLS.

22 Click on the OK button. The VPLS Service (Create) form closes.

23 Close the Manage Services form.

Procedure 68-61 To enable SPB on a control B-VPLS site

Perform the following procedure to enable SPB on the B-VPLS and configure the B-site as a control B-VPLS.



Note — All of the B-sites in the VPLS must be configured as control B-VPLS sites.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Select the required VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, right-click on the B-site and choose Properties. The VPLS Site (Edit) form opens with the General tab displayed.

5 Click on the Backbone tab. The General tab is displayed.

6 Click on the SPB tab.

7 Configure the SPB Mode parameter by choosing the Control B-VPLS option.

8 Click on the Create button in the SPB Instance for Control Service panel. The SPB (Create) form opens with the General tab displayed.



Note — The SPB instance configuration, except the ISIS instance and the Bridge Priority parameter on the Level 1 tab, must be identical on all the sites in a control B-VPLS.

9 Configure the parameters:

- ISIS Instance
- Forwarding Identifier (FID)
- Administrative State
- Automatic Enable Interface

10 Configure the parameters in the ISIS panel:

- LSP Life Time (seconds)
- LSP Wait (seconds)
- LSP Initial Wait (seconds)
- LSP Second Wait (seconds)
- SPF Wait (seconds)
- SPF Initial Wait (milliseconds)
- SPF Second Wait (milliseconds)
- Overload
- Overload Timeout (seconds)
- Overload On Boot
- Overload On Boot Timeout (seconds)

The Overload Timeout (seconds) parameter is configurable only if the Overload parameter is set to Enabled.

The Overload On Boot Timeout (seconds) parameter is configurable only if the Overload On Boot parameter is set to Enabled.

11 Click on the Level 1 tab.

12 Configure the parameters:

- Bridge Priority
- Unicast Forwarding Tree Topology

13 Create the ECT-to-FID range mapping.

i Click on the ECT Algorithm to FID Range Mappings tab.

ii Click on the Create button. The ECT Algorithm to FID Range Mapping (Create) form opens.

iii Configure the parameters:

- FID Range Start
- FID Range End
- FID Range Algorithm

iv Click on the OK button. The ECT Algorithm to FID Range Mapping (Create) form closes and a dialog box appears.

v Click on the OK button.

vi Repeat steps i to v, as required.



Note — The ECT-to FID range mapping parameter values must be identical on all the sites in the control SPB B-VPLS. In addition, each site must have the same number of ECT-to-FID range mapping objects.

14 Create the IS-IS interface, or SPB link, of an access interface if you have not enabled the Automatic Enable Interface parameter.



Note — If you enabled the Automatic Enable Interface in step 9, all of the L2 access interfaces on the site and all of the L2 access interfaces that are subsequently created on the B-site are automatically enabled for SPB.

i Click on the Access Interfaces tab.

ii Click on the Create button. The Access Interface, ISIS Instance (Create) form opens with the General tab displayed.

iii Click on the Select button in the SAP panel to select the L2 access interface. The Select SAP - Access Interface - ISIS Instance form opens.

iv Select an L2 access interface and click on the OK button. The Select SAP - Access Interface - ISIS Instance form closes.

v Configure the Description parameter.

vi Configure the Administrative State to specify the administrative state for SPB on the SAP.

vii Click on the Behavior tab and configure the parameters:

- LSP Pacing Interval (seconds)
- Retransmit Interval (seconds)

viii Click on the Level 1 tab and configure the parameters:

- Hello Interval (seconds)
- Hello Multiplier
- Metric

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Access Interface, ISIS Instance (Create) form closes.

15 Configure SPB on the B-VPLS spoke SDP binding if you have not enabled the Automatic Enable Interface parameter.



Note — If you enabled the Automatic Enable Interface in step 9, all of the spoke SDP bindings on the site and all of the spoke SDP bindings that are subsequently created on the B-site are automatically enabled for SPB.

i Click on the SDP Binding tab.

ii Click on the Spoke SDP Bindings tab.

iii Click on the Create button. The Spoke SDP Binding Interface, ISIS Instance (Create) form opens with the General tab displayed.

iv Click on the Select button in the Circuit panel to select the spoke SDP binding. The Select Circuit - Spoke SDP Binding Interface - ISIS Instance form opens.

v Select a circuit and click on the OK button. The Select Circuit - Spoke SDP Binding Interface - ISIS Instance form closes.

vi Configure the Description parameter.

vii Configure the Administrative State to specify the administrative state for SPB on the spoke SDP binding.

viii Click on the Behavior tab and configure the parameters:

- LSP Pacing Interval (seconds)
- Retransmit Interval (seconds)

ix Click on the Level 1 tab and configure the parameters:

- Hello Interval (seconds)
- Hello Multiplier
- Metric

x Click on the OK button. A dialog box appears.

xi Click on the OK button. The Spoke SDP Binding Interface, ISIS Instance (Create) form closes.

16 Click on the OK button. The SPB - ISIS Instance (Create) form closes.

17 Click on the OK button. The Site - VPLS Service (Edit) form closes.

18 Close the VPLS Service (Edit) form.

19 Close the Manage Services form.



Note — You can perform an RCA audit on the SPB control B-VPLS to verify the configuration. See Procedure 80-3 for more information and Table 80-1 for a description of probable causes.

Procedure 68-62 To enable SPB on a user B-VPLS site

Perform the following procedure to enable SPB on the B-VPLS and configure the B-site as a user B-VPLS. A control SPB B-VPLS service must already exist. See Procedure 68-61 for more information about how to create a control SPB B-VPLS.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Select the required VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, right-click on the B-site and choose Properties. The VPLS Site (Edit) form opens with the General tab displayed.

5 Click on the Backbone tab. The General tab is displayed.

6 Click on the SPB tab.

7 Set the SPB Mode parameter to User B-VPLS.

8 Click on the Select button in the User Service panel to associate the user B-VPLS with a control B-VPLS. The Select Association with Control B-VPLS Site form opens.

9 Select a B-site and click on the OK button. The Select Association with Control B-VPLS Site form closes.



Note — You must select the same control B-VPLS for all the sites in a user B-VPLS.

10 Configure the Forwarding Identifier (FID) parameter.



Note — The Forwarding Identifier (FID) parameter must be the same for all the user B-VPLS sites within the SPB B-VPLS.

11 Click on the OK button. The VPLS Site (Edit) form closes.

12 Close the VPLS Service (Edit) form.

13 Close the Manage Services form.



Note — You can perform an RCA audit on the SPB user B-VPLS service to ensure a correct configuration. See Procedure 80-3 for more information and Table 80-1 for a description of probable causes.

Procedure 68-63 To view SPB fate-shared objects

Perform the following procedure to list all of the SPB-enabled B-VPLS SAPs, spoke SDP bindings, and user B-VPLS sites that are fate-shared.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Select the required VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, right-click on the B-site and choose Properties. The VPLS Site (Edit) form opens with the General tab displayed.

5 Click on the SBP Fate Sharing tab. The SAPs tab is displayed with a list of fate-shared SAPs within the SPB B-VPLS.

6 Click on the Spoke SDPs tab. A list of fate-shared spoke SDP bindings within the SPB B-VPLS is displayed.

7 Click on the SPB User Sites tab. A list of SPB user B-VPLS sites associated with the control B-VPLS is displayed.

8 Close the VPLS Site (Edit) form.

9 Close the VPLS Service (Edit) form.

10 Close the Manage Services (Edit) form.

Procedure 68-64 To view SPB instances on an NE

Perform the following procedure to list all of the SPB instances associated with an NE.

1 Right-click on an NE in the Equipment navigation tree and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

2 Click on the Globals tab. The Load Balancing tab is displayed.

3 Click on the Service tab. The General tab is displayed.

4 Click on the SPB Control Instances tab. A list of all SPB instances configured on the NE is displayed.

5 Close the Network Element (Edit) form.

Procedure 68-65 To create an I-VPLS

1 Choose Create→Service→VPLS from the 5620 SAM main menu. The VPLS Service (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the VPLS. The Select Customer - VPLS Service form opens.

3 Select a customer for the VPLS and click on the OK button. The Select Customer - VPLS Service form closes, and the VPLS Service (Create) form displays the customer information.

4 Configure the parameters:

- Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Auto-Assign ID
- SVC Mgr Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Service Name
- Description
- Service Tier
- Service Priority
- Administrative State
- Default Mesh VC ID
  This parameter is configurable when the Inherit Service ID Value parameter is disabled.
- Inherit Service ID Value
- Automatic Mesh SDP Binding Creation
- Profile Name
  This parameter is configurable when the Automatic Mesh SDP Binding Creation parameter is enabled.
- Transport Type
  This parameter is configurable when the Automatic Mesh SDP Binding Creation parameter is enabled and the Profile Name parameter is left blank.

5 Configure the OLC state:

i Click on the Apply button.

ii Configure the parameters:

- Current OLC State
- Revert OLC State

6 To configure service tunnel required bandwidth for the service, perform the following steps.



Note — In order to configure service tunnel required bandwidth, you must enable multi-segment tunnel selection and service bandwidth management at the system level.

i Click on the Bandwidth tab.

ii Configure the Bandwidth Method parameter.

iii If the Bandwidth Method parameter is set to Manual or Calculate, configure LSP Path Booking parameter.

iv If the Bandwidth Method parameter is set to Manual, enter a required bandwidth value for each CoS (see Override Service Configuration).

7 Perform one of the following.

a Create an I-site for the VPLS. Go to step 8.

b Complete service creation if I-sites, I-L2 access interfaces, and SDP bindings for the VPLS are to be created later. Go to step 27.

8 On the navigation tree, right-click on Sites and choose Create VPLS I-Site from the contextual menu. The Select Network Elements - VPLS form opens with a list of available sites.

9 Select a site and click on the OK button. The I-Site (Create) form opens with the General tab displayed.

10 Configure the parameters:

- Name
- Description
- MTU
- Administrative State
- Monitor Access Interface Operational State
- Per Service Hashing for LAG Enabled
- Tunnel Fault Notification

Tunnel Fault Notification is configurable on sites where the device has ports configured in access or hybrid mode with QinQ encapsulation.

If you are configuring a tunnel facility MEP, Tunnel Fault Notification must be set to Accept, in order to accept the fault propagation from the tunnel facility MEP.

11 Click on the Backbone tab.

12 Select the Backbone VPLS site.

i Click on the Select button. The Select Backbone VPLS Site - I-Site form is displayed.

ii Click on the Search button. A list with all the B-VPLSs that can be used by the I-VPLS is displayed. You can narrow the search by using the using the filtered properties shown in the form. Only B-VPLSs that are present in PEs that have the I-Sites of the VPLS is shown.

iii Select a B-VPLS and click on the OK button. The Select Backbone VPLS Site - I-Site form closes and the Service ID of the chosen B-VPLS appears on the I-Site (Create) form.



Note — The selection of the B-site in this step must be repeated for each I-site you create, since you must select the B-VPLS site that is within the same site as the I-site.

13 Configure the parameters:

- Send Flush All From Me
- Send Flush All But Mine
- Administrative ISID
- Backbone STP
- Force Q Tag Forwarding



Note 1 — The Force Q Tag Forwarding parameter is only displayed if the NE for this site is in chassis mode D or higher or Sparrow.

Note 2 — Only the Administrative ISID and Backbone STP parameters are applicable when configuring PBB on a 7210 SAS-M or a 7210 SAS-X.

14 Configure MFib, STP, FIB, and MAC Protection parameters for the I-site, if required.

i Click on the Forwarding Control tab. The MFib tab is displayed.

ii Configure the parameters:

- Table size (entries)
- High Watermark (%)
- Low Watermark (%)

iii Click on the STP tab to configure STP parameters for the I-site, if required. Otherwise, go to step v.

iv Configure the bridge-level STP parameters for the I-site.

Alcatel-Lucent STP in a VPLS interoperates with customer STP implementations as a mechanism for loop detection and prevention. The bridge-level parameters balance the STP resiliency and speed of convergence. Modifying the bridge-level parameters must be done within the constraints of the following formulas:

- 2 × (Bridge Forward Delay – 1.0 s) >= Bridge Max Age
- Bridge Max Age >= 2 × (Bridge Hello Time + 1.0 s)



Note 1 — If you are configuring an MVPLS I-site, set the STP Mode parameter to RSTP or MSTP, depending on the MVPLS type. The MSTP option is available only if you are creating an MVPLS. See Procedure 68-59 for more information about creating an MVPLS.

Note 2 — MSTP is configurable only on the 7450 ESS, 7710 SR, 7750 SR, and 7950 XRS.

- Bridge Forward Delay (seconds)
- Bridge Hello Time (seconds)
- Bridge Max Age (seconds)
- Priority
- STP Mode
- Maximum BPDUs (PDUs/Hello Interval)
- Administrative State

v Click on the FIB tab to configure FIB parameters for the I-site, if required. Otherwise, go to step 19.

vi Configure the parameters:

- High Watermark (%)
- Low Watermark (%)
- Local Age Time (seconds)
- Remote Age Time (seconds)
- Size (entries)
- Aging Enabled
- Learning Enabled
- Discard Unknown Destinations
- MAC Flush on fail
- Propagate MAC Flush

vii Depending on the type of device being configured, the Mac Move panel appears. Configure the MAC move parameters, if required:

- Move Frequency
- Retry Timeout
- Number of Retries
- Administrative State
- Primary Ports Cumulative Factor
- Secondary Ports Cumulative Factor

viii Click on the MAC Protection tab to configure the list of protected MAC addresses.

ix Click on the Create button. The MAC Protection (Create) form opens.

x Configure the Protected Mac Address parameter.

xi Click on the OK button to close the form and add the MAC address to the list of protected MAC addresses.

xii If you are configuring an MVPLS I-site that requires MSTP, click on the MSTP tab. Otherwise, go to step 18.



Note — MSTP is configurable only on the 7450 ESS, 7710 SR, 7750 SR, and 7950 XRS.

xiii Configure the parameters:

- Region Name
- Region Revision
- Bridge Max Hops

xiv Click on the MST Instances tab.

xv Click on the Create button. The MST Instance (Create) form opens with the General tab displayed.

xvi Configure the parameters:

- Instance Index
- Priority

xvii Click on the VLAN Ranges tab. Click on the Create button. The MST Instance Managed VLAN range (Create) form opens.

xviii Configure the parameters:

- Min. VLAN Tag
- Max. VLAN Tag

xix Click on the OK button. The MST Instance Managed VLAN Range (Create) form closes, and a dialog box appears.

xx Click on the OK button. The MST Instance (Create) form refreshes with the new managed VLAN range.

xxi Click on the OK button. The MST Instance (Create) form closes and a dialog box appears.

xxii Click on the OK button. The MVPLS Site (Create) form refreshes with the new MST instance.

15 Configure ingress multicast forwarding, if required.



Note — An Operational Channels tab appears when you access the VPLS I-Site form in the Edit mode. It displays data for the operational channels when traffic from a specific multicast source for a specific multicast group passes through the service. You must click on the Search button to refresh the data. See chapter 42 for information about listing the operational channel parameters.

i Click on the Multicast tab.

ii Click on the Mcast Path Mgmt tab.

iii Click on the Select button to choose a multicast info policy. The Select Ingress Info Policy form opens.

iv Select a policy in the list and click on the OK button. The Select Ingress Info Policy form closes and the policy identifier is displayed on the Site (Create) form.

16 To configure service tunnel required bandwidth for the site, perform the following steps.



Note — In order to configure service tunnel required bandwidth, you must enable multi-segment tunnel selection and service bandwidth management at the system level.

i Click on the Bandwidth tab.

ii Enable the Override Service Configuration parameter.

iii Configure the Bandwidth Method parameter.

iv If the Bandwidth Method parameter is set to Manual, enter a required bandwidth value for each CoS (see CoS 0 Bandwidth - CoS 7 Bandwidth).

17 Configure IGMP snooping for the site, if required.

i Click on the Multicast tab.

ii Click on the IGMP Snooping tab.

iii Configure the parameters:

- Administrative State
- Query Interval (seconds)
- Robust count
- Report source address
- Use query source address
- Query source address

The Query source address parameter is configurable when the Use query source address parameter is enabled.

18 If you are configuring an MVPLS I-site, go to step 20.

19 Configure an SHG on the site, if required.



Note — You must configure an SHG or RSHG if you plan to create a spoke circuit from this VPLS I-site to a VLL or to another VPLS.

i Click on the Split Horizon Groups tab.

ii Click on the Create button. The Site, New Split Horizon Group (Create) form opens.

iii Configure the parameters:

- Name
- Description
- Restrict Protected Source
- Restrict Protected Source Action
- Restrict Unprotected Destination

iv Click on the OK button. The Site, New Split Horizon Group (Create) form closes.

20 To create an I-L2 access interface for the I-site, perform steps 4 to 32 of Procedure 68-70.

21 To create a spoke SDP binding between the I-site and regular VPLS sites, click on the Components tab and perform steps 9 to 40 of Procedure 68-44, as required. I-sites can only use spoke SDP bindings.



Note 1 — You cannot create a spoke SDP binding on an MVPLS site that runs MSTP, or enable MSTP on a site that has a spoke SDP binding.

Note 2 — You cannot enable MSTP on an access interface that has a non-zero encapsulation value.

22 Click on the OK button. The I-Site (Create) form closes, and a dialog box appears.

23 Click on the OK button. The VPLS Service (Create) form displays the new I-site on the navigation tree under VPLS.

24 Repeat steps 8 to 23 to create additional I-sites for the I-VPLS.

25 Add protected MAC addresses at the service level, if required. Protected MAC addresses that you add on the site level, as performed in step 14, are automatically added to the service-level MAC protection list.

i Click on the Forwarding Control tab.

ii Click on the MAC Protection tab.

iii Click on the Create button. The MAC Protection (Create) form opens.

iv Configure the Protected Mac Address parameter.

v Click on the OK button. The MAC Protection (Create) form closes and the protected MAC address is listed on the VPLS Service (Create) form.

26 To configure bandwidth for the service if required, click on the Bandwidth tab. The Required Bandwidth tab is displayed. Proceed as follows:



Note 1 — The Bandwidth tab is only available if service CAC is configured. See "To configure service CAC to automatically bind PBB tunnels" in the *5620 SAM System Administrator Guide* for information about enabling and disabling service CAC.

Note 2 — The ability to configure required bandwidth is only applicable to I-sites.

i For each CoS, enter the value for the CoS Bandwidth (Mbps), as required.

ii Click on the General tab to determine the CAC status.

If the Verify CAC button is enabled, the CAC has not been verified. The Probable Cause and CAC Status fields provide details.

The CAC Status field describes the current CAC status of the service. CAC statuses are as follows.

- CAC Verified indicates that all tunnels have sufficient bandwidth to admit service and that requested bandwidth for the service is booked on the appropriate physical links.
- CAC Failed indicates that the attempt made to admit service into the network was unsuccessful. The most likely cause for this is insufficient bandwidth. See the Probable Cause field for more specific information.
- BW Defined, No CAC Request indicates that the required bandwidth is defined on the service; however, a CAC request has not occurred.
- CAC To be Verified indicates that a tunnel has been configured on the service either manually or through the CLI; however, the required bandwidth has not been verified in the network.

The Probable Cause field describes possible reasons for the current CAC state. Probable causes are as follows.

- No Candidate Tunnels Found indicates that the autobind tunnel function was found, but no suitable tunnels were found.
- Different PBB Tunnels Applied to Service indicates that two or more different PBB tunnels are configured on this service.
- Not Enough Bandwidth on any Candidate Tunnels indicates that one or more candidate tunnels were found, but the available bandwidth was insufficient to admit the service.
- Automatic PBB Tunnel Selection Failed indicates that a suitable PBB tunnel was found, but there were errors when attempting to assign the tunnel to the service. A dialog box will provide more details.
- Site Missing Tunnel indicates that at least one selected site is not configured with a PBB tunnel.
- All PBB Tunnels have not been Verified indicates that all sites within the service have a tunnel configured, but the available bandwidth has not been booked or verified in the network.

iii To manually verify the CAC, click on the Verify CAC button if it is enabled. The 5620 SAM will attempt to find the most appropriate PBB tunnel for the service based on available bandwidth, and to automatically bind the tunnel to the service if one has not already been assigned.

27 Click on the OK button. The VPLS Service (Create) form closes.

28 Close the Manage Services form.

Procedure 68-66 To create a VPLS or MVPLS B-L2 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site to which you want to add the access interface; expand the entries for that site.

5 Right-click on L2 Access Interfaces and choose Create B-L2 Access Interface. The B-L2 Access Interface (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Description
- Administrative State
- MC Ring Node
- Tunnel Fault Notification

Tunnel Fault Notification is configurable on interfaces where the device has ports configured in access or hybrid mode with QinQ encapsulation.

If you are configuring a tunnel facility MEP, Tunnel Fault Notification must be set to Accept, in order to accept the fault propagation from the tunnel facility MEP.

7 Choose a transit prefix policy for the interface, if required.

i Click on the Select button in the Transit Prefix Policy panel. The Select Transit Prefix Policy - B-L2 Access Interface form opens.

ii Select a transit prefix policy and click on the OK button.

8 Choose an SHG for the interface, if required.

i Click on the Select button in the Split Horizon Group panel. The Select Split Horizon Group Name - B-L2 Access Interface form opens.



Note — You must configure an SHG or residential SHG for a VPLS if you plan to create a spoke circuit from this VPLS site to a VLL or another VPLS.

ii Select an SHG and click on the OK button. The Select Split Horizon Group Name - B-L2 Access Interface form closes, and the B-L2 Access Interface (Create) form refreshes with the SHG name.

9 Click on the Port tab.

10 Click on the Select button to choose a port for the B-L2 access interface. The Select Terminating Port - VPLS B-L2 Access Interface form opens.



Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

11 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - VPLS B-L2 Access Interface form closes, and the VPLS B-L2 Access Interface (Create) form displays the port information.

12 Configure the parameters:

- Outer Encapsulation Value
- Inner Encapsulation Value



Caution — The creation of a SAP that uses the same port and encapsulation values as an existing inactive MSAP fails under the following conditions:

- If you try to use the 5620 SAM to create a SAP, the configuration fails and the 5620 SAM displays an error message.
- If you use a CLI to create a SAP in a service other than the service that contains the MSAP, the configuration succeeds but the MSAP is inactive until the regular SAP is deleted. Although the 5620 SAM displays the SAP and MSAP, the MSAP remains inactive and consumes resources.
- If you use a CLI to create a SAP in the service that contains the MSAP, the SAP creation fails.

Alcatel-Lucent recommends that you delete an inactive MSAP from the 5620 SAM if you need to create a regular SAP on the same port using the same encapsulation values. See Procedure 65-34 for more information about deleting MSAPs.

For a B-L2 access interface, only Null, dot1q, and QinQ encapsulation are supported.

When the selected port uses dot1q encapsulation, you can enable the Auto-Assign ID parameter to have the Outer Encapsulation Value parameter automatically assigned. If you choose this, the system assigns the lowest unused encapsulation value.



Note — You can set the Auto-Assign ID parameter to be the default parameter for dot1q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter in the User Preferences form. Choose Application→ User Preferences from the main menu.

13 Depending on the port that you have chosen, the Egress Multicast Group tab is configurable. Configure the EMG, if required.

i Click on the Egress Multicast Group tab. The Select Egress Multicast Group-B-L2 Access Interface form opens.

ii Select an EMG and click on the OK button. The Select Egress Multicast Group-B-L2 Access Interface form closes, and the Egress Multicast Group tab refreshes with the EMG name.



Note — The Egress Multicast Group-L2 Interface form lists only EMGs that have the same egress filter and encapsulation type as the interface.

14 If the selected port uses FR encapsulation, configure Frame Relay for the interface.

i Click on the Frame Relay tab.

ii Set the FRF-12 Mode parameter to Enabled.

iii Configure the parameters:

- FRF-12 End-To-End Fragment Threshold
- Scheduling Class
- Fragment Interleave

15 Assign ingress and egress QoS policies to the interface, if required.

i Click on the QoS tab.



Note — Items such as policies, schedulers, and filters can be applied later to multiple service components at once by selecting and right-clicking the components in the service navigation tree, choosing Properties, and configuring the parameters on the appropriate tab. This action opens a properties form in a new window for the component that was right-clicked. The navigation tree is not displayed in this new window.

ii Configure the Ingress Match QinQ Dot1P parameter.

The Ingress Match QinQ Dot1P parameter is configurable only when the encapsulation type of the port is dot1q or QinQ.

iii Click on the Select button in the Ingress Policy panel to choose an ingress QoS policy. The Select Ingress Policy - B-L2 Access Interface form opens.

iv Select an ingress QoS policy and click on the OK button. The Select Ingress Policy - B-L2 Access Interface form closes, and the B-L2 Access Interface (Create) form refreshes with the ingress QoS policy name.



Note — If you select an access ingress policy that has a forwarding class mapped to an ingress queue group, the port that you choose for the VPLS L2 access interface must use the same access ingress queue group.

See Procedure 16-1 for information about configuring Ethernet ports. See chapter 42 for information about queue group template policies.

v Click on the Ingress Queue Group Template Policy Select button in the Forwarding Plane Redirect panel to choose a policy. The Select Forwarding Plane Queue Group Instance form opens.

vi Choose a policy from the list and click on the OK button. The Select Forwarding Plane Queue Group Instance form closes. The VPLS L2 Access Interface (Create) form refreshes with the Ingress Queue Group Template Policy information displayed.

vii Configure the Instance ID parameter.

viii Configure the Egress Mark QinQ Top Bits Only parameter.

The Egress Mark QinQ Top Bits Only parameters are configurable only when the encapsulation type of the port is dot1q or QinQ.

ix Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - B-L2 Access Interface form opens.

x Select an egress QoS policy and click on the OK button. The Select Egress Policy - B-L2 Access Interface form closes, and the B-L2 Access Interface (Create) form refreshes with the egress QoS policy name.



Note — If you select an access egress policy that has a forwarding class mapped to an egress queue group, the port that you choose for the VPLS L2 access interface must use the same access egress queue group.

See Procedure 16-1 for information about configuring Ethernet ports. See chapter 42 for information about queue group template policies.

xi If the port you selected in step 10 is not an HSMDA port then go to step 16.

xii Configure the Packet Byte Offset (bytes) parameter, if required. Before you can configure the parameter, you must select the associated Override check box.

xiii Click on the Select button in the Egress HSMDA Override panel to choose a WRR policy. The Select WRR Policy form opens.

xiv Choose a WRR policy and click on the OK button. The Select WRR Policy form closes and the VPLS L2 Access Interface (Create) form reappears with the WRR policy information displayed.

xv Click on the Select button in the Egress HSMDA Override panel to choose an HSMDA egress secondary shaper policy. The Select Secondary Shaper form opens.

xvi Choose a secondary shaper and click on the OK button. The Select Secondary Shaper form closes and the VPLS L2 Access Interface (Create) form reappears with the secondary shaper information displayed.

xvii Configure the parameters:

- Use Shared Queue
- Use Multipoint Shared Queue

16 Click on the Schedulers tab to configure scheduling; otherwise, go to step 18.



Note — The Schedulers tab is configurable only when a port is assigned to the interface.

17 Perform one of the following.

a Specify that an aggregation scheduler policy is not applied to the interface.

i Set the Aggregation parameter to off.



Note — The Aggregation parameter is not configurable if the port you selected in step 10 is an HSMDA port.

ii Configure the parameters:

- Aggregate Rate Limit (kbps)
- Frame-Based Accounting



Note 1 — The Aggregate Rate Limit (kbps) and Frame-Based Accounting parameters are configurable only when there is no scheduler specified in the Egress Scheduler panel.

Note 2 — The Frame-Based Accounting parameter is not configurable if the port you selected in step 10 is an HSMDA port.

Note 3 — You cannot specify an egress scheduler when the Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

iii Click on the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - B-L2 Access Interface form opens.

iv Select an ingress scheduler and click on the OK button. The Select Ingress Scheduler - B-L2 Access Interface form closes, and the B-L2 Access Interface (Create) form refreshes with the ingress scheduler information displayed.

v Click on the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Policer Control Policy form opens.

vi Choose a policer control policy and click on the OK button. The Select Policer Control Policy form closes and the VPLS B-L2 Access Interface (Create) form reappears with the ingress policer control policy information displayed.

vii If the port you selected in step 10 is an HSMDA port, go to step 18.

viii Click on the Select button in the Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - B-L2 Access Interface form opens.

ix Select an egress scheduler and click on the OK button. The Select Egress Scheduler - B-L2 Access Interface form closes, and the B-L2 Access Interface (Create) form refreshes with the egress scheduler information displayed.

x Click on the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Policer Control Policy form opens.

xi Choose a policer control policy and click on the OK button. The Select Policer Control Policy form closes and the VPLS B-L2 Access Interface (Create) form reappears with the egress policer control policy information displayed.

xii Go to step 18.

b Specify that an access scheduler policy is applied to the interface.



Note — You cannot specify an access scheduler policy if the port you selected in step 10 is an HSMDA port. Go to step 18.

i Set the Aggregation parameter to on.

ii Configure the Frame-Based Accounting parameter.

iii Click on the Select button in the Aggregation Scheduler panel to choose an aggregation scheduler. The Select Aggregation Scheduler - B-L2 Access Interface form opens.

iv Select an aggregation scheduler and click on the OK button. The Select Aggregation Scheduler - B-L2 Access Interface form closes, and the B-L2 Access Interface (Create) form refreshes with the aggregation scheduler information displayed.

18 Assign ingress and egress ACL filters to the interface, if required.



Note — Only MAC filters are allowed for B-L2 Access Interfaces.

i Click on the ACL tab.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - B-L2 Access Interface form opens.

iii Select an ingress ACL filter and click on the OK button. The Select Ingress Filter - B-L2 Access Interface form closes, and the B-L2 Access Interface (Create) form refreshes with the ingress ACL filter name.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - B-L2 Access Interface form opens.

v Select an egress ACL filter and click on the OK button. The Select Egress Filter - B-L2 Access Interface form closes, and the B-L2 Access Interface (Create) form refreshes with the egress ACL filter name.

19 Assign an accounting policy to the interface, if required.

i Click on the Accounting tab.

ii Configure the Collect Accounting Statistics and Ingress Counter Type parameters.

iii Click on the Select button to choose an accounting policy. The Select Accounting Policy - B-L2 Access Interface form opens.

iv Select an accounting policy and click on the OK button. The Select Accounting Policy - B-L2 Access Interface form closes, and the B-L2 Access Interface (Create) form refreshes with the accounting policy name.

20 Configure BPDU Termination, STP, FIB, and MRP parameters for the interface, if required.

i Click on the Forwarding Control tab. Depending on the device being configured, the BPDU Termination tab is displayed. Otherwise, go to step iii.

ii Configure the parameters:

- L2 Protocol Termination

  When the L2 Protocol Termination parameter is set to Enabled, a list of L2PT protocols is displayed. Select all that are required.
- BPDU Translation
- Force L2PT on Managed L2 Access Interface

  The Force L2PT on Managed L2 Access Interface parameter is only available for MVPLS B-L2 access interfaces. When the Force L2PT on Managed L2 Access Interface parameter is set to Enabled, a list of L2PT protocols is displayed. Select all that are required.

iii Click on the STP tab.

iv Configure the parameters:

- Path Cost
- Port Number
- Priority
- Edge Port
- Edge Capability Detection
- Link Type
- Root Guard
- Administrative State

v Click on the FIB tab.

vi Configure the parameters:

- Aging Enabled
- Learning Enabled
- Limit Mac Move
- Limit Mac Move Level
- Discard Unknown Source

vii If you are creating an MVPLS to run MSTP, the MST Instances tab is configurable. Otherwise, go to step xiv.

viii Click on the MST Instances tab to edit a SAP MST instance.

ix Select an MST instance and click on the Properties button.

x The B-L2 Access Interface MST Instance (Edit) form opens. Configure the parameters:

- Path Cost
- Priority

xi Click on the OK button to close the B-L2 Access Interface MST Instance (Edit) form. A dialog box appears.

xii Click on the OK button. The B-L2 Access Interface (Create) form refreshes with the new MST instance.

xiii If you are configuring an MVPLS B-L2 access interface, go to step 21.

xiv Click on the MRP tab.

xv Configure the parameters:

- MRP Join Time (tenths of a second)
- MRP Leave Time (tenths of a second)
- MRP Leave All Time (tenths of a second)
- MRP Periodic Time (tenths of a second)
- MRP Periodic Enabled



Note — You can view information regarding MMRP Entries by clicking on the MMRP tab.

xvi Click on the Select button to select an PBB MRP Policy. The Select PBB MRP Policy form opens.

xvii Choose the desired policy and click OK.

21 Assign a DoS protection policy to the interface, if required.



Note — A default DoS protection policy is automatically assigned to the interface.

i Click on the Security tab.

ii Click on the Select button. The Select NE DoS Protection - B-L2 Access Interface form opens.

iii Select a DoS protection policy in the list and click on the OK button. The Select NE DoS Protection - B-L2 Access Interface form closes and the policy ID is displayed on the B-L2 Access Interface (Create) form.

iv Configure the MAC Monitoring parameter.

22 Configure a redundant VLAN range, if required.



Note — If an MVPLS site has SAPs that manage traffic on the associated VPLS SAPs, you must define a redundant VLAN range during SAP creation. The redundant VLAN range defines the range of VC IDs for VPLS SAPs that the MVPLS manages.

i Click on the Redundancy tab.

ii Click on the Create button. The RedundantVlanRange (Create) form opens.

iii Configure the parameters:

- Min VLAN ID
- Max VLAN ID

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The B-L2 Access Interface (Create) form refreshes with the redundant VLAN range entry.

23 Configure anti-spoofing filters for the interface, if required.

i Click on the Anti-Spoofing tab.

ii Configure the MAC Pinning parameter.

24 Specify the queue overrides.

i Click on the Override Policy Items tab.



Note — The Override Policy Items tam contains a number of tabs. However, the tabs that are displayed depend on the port type that you have chosen for this interface.

- If you configured a non-HSMDA port, then the Access Ingress Queues, Access Egress Queues, Ingress Policer, and Egress Policer tabs are active.
- If you configured an HSMDA port, then the Access Ingress Queues, Access Egress HSMDA Queues and Ingress Policer tabs are active.

ii See Procedure 43-42 for information about setting queue overrides.

25 Associate a MEP with the B-L2 Access interface, if required.

i Click on the ETH-CFM tab.

ii Perform steps 8 to 27 in Procedure 68-37.

26 Assign an ANCP policy to the interface, if required.

i Click on the ANCP Static Map tab. The ANCP Static Map (Create) form opens.

ii Configure the ANCP String parameter.

iii Click on the Select button to choose an ANCP Policy. The Select ANCP Policy - ANCP Static Map form opens.

iv Select an ANCP policy and click on the OK button. The Select ANCP Policy - ANCP Static Map form closes and the ANCP Static Map form reappears with the ANCP policy information displayed.

v Click on the OK button. The ANCP Static Map form closes.

27 Click on the OK button. The B-L2 Access Interface (Create) form closes and a dialog box appears.

28 Click on the Yes button. The VPLS Service (Edit) form reappears.

29 Repeat steps 4 to 28 for each additional B-L2 access interface that you want to create.

30 Click on the OK button. A dialog box appears.

31 Click on the Yes button. The VPLS Service (Edit) form closes.

32 Close the Manage Services form.

Procedure 68-67 To create a static ISID range on a VPLS B-L2 access interface or spoke SDP binding

Perform the following procedure to create a static ISID range to allow I-VPLS services to connect to non-SPB I-VPLS services. You can create one or more static ISID ranges on a B-L2 access interface or spoke SDP binding on a control or user B-VPLS site. See Procedures 68-61 and 68-62 for information about how to enable SPB on a control or user site.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, expand the B-VPLS site.

5 Perform one of the following:

a To add a static ISID range on a B-L2 access interface, expand the L2 Access Interfaces icon, and click on the B-L2 access interface. The Port (Edit) form opens with the General tab displayed.

b To add a static ISID range on an SDP binding, expand the Spoke SDP Bindings icon and click on the SDP binding. The Spoke SDP Binding (Edit) form opens with the General tab displayed.

6 Click on the Static ISID tab. The Static ISID Ranges tab is displayed.

7 Click on the Create button. The Static ISID Range Entry (Create) form opens.

8 Configure the parameters:

- Entry ID
- From ISID
- To ISID

9 Click on the OK button. The Static ISID Range Entry (Create) form closes.

10 To create additional range entries, repeat steps 7 to 9.

11 To view the status information about the configured static ISIDs, click on the Static ISID Ranges tab.

12 Click on the OK button. The Port (Edit) form or the Spoke SDP Binding (Edit) form closes and a dialog box appears.

13 Click on the Yes button. The VPLS Service (Edit) form reappears.

14 Click on the OK button. A dialog box appears.

15 Click on the Yes button. The VPLS Service (Edit) form closes.

16 Close the Manage Services form.

Procedure 68-68 To create a static B-MAC on a B-VPLS site

Perform the following procedure to create a static B-MAC to allow remote PBB Epipe VLL services to connect to an SPB network. You can create a static B-MAC on a B-L2 access interface or spoke SDP binding on a control or user B-VPLS site. See Procedures 68-61 and 68-62 for information about how to enable SPB on a control or user site.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the B-VPLS site. The Site (Edit) form opens with the General tab displayed.

5 Click on the Static MACs tab.

6 Click on the Create button. The Conditional Static MAC (Create) form opens.

7 Configure the MAC Address parameter.

8 Perform one of the following:

a Choose a SAP.

i Click on the Select button in the SAP panel. The Select SAP - Conditional Static MAC form opens with a list of SAPs.

ii Choose a SAP and click on the OK button. The Select SAP - Conditional Static MAC form closes.

b Choose a spoke SDP binding.

i Click on the Select button in the Spoke SDP Binding panel. The Select Spoke SDP Binding - Conditional Static MAC form opens with a list of spoke SDP bindings.

ii Choose an SDP binding and click on the OK button. The Select Spoke SDP Binding - Conditional Static MAC form closes.

9 Click on the OK button. The Conditional Static MAC (Create) form closes.

10 To create additional static B-MACs, repeat steps 6 to 9.

11 Click on the OK button. The Site (Edit) form closes and a dialog box appears.

12 Click on the Yes button. The VPLS Service (Edit) form reappears.

13 Click on the OK button. A dialog box appears.

14 Click on the Yes button. The VPLS Service (Edit) form closes.

15 Close the Manage Services form.

Procedure 68-69 To create an ISID policy on a control or user B-VPLS site

Perform the following procedure to create an ISID policy. An ISID policy defines a group of actions for individual ISIDs or ISID ranges. You can define whether the default multicast tree is used and whether the advertisement of ISIDs in SPB is supressed when I-VPLS or static ISIDs are used for unicast services. See Procedures 68-61 and 68-62 for information about how to enable SPB on a control or user site.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the B-VPLS site. The Site (Edit) form opens with the General tab displayed.

5 Click on the ISID Policy tab.

6 Click on the Create button. The ISID Policy Range Entry (Create) form opens.

7 Configure the parameters:

- Entry ID
- From ISID
- To ISID
- Use Default Multicast Tree
- Advertise Local

You cannot set the Use Default Multicast Tree and the Advertise Local parameters to False at the same time.

8 Click on the OK button. The ISID Policy Range Entry (Create) form closes.

9 To create additional policies, repeat steps 6 to 8.

10 Click on the OK button. The Site (Edit) form closes and a dialog box appears.

11 Click on the Yes button. The VPLS Service (Edit) form reappears.

12 Click on the OK button. A dialog box appears.

13 Click on the Yes button. The VPLS Service (Edit) form closes.

14 Close the Manage Services form.

Procedure 68-70 To create a VPLS I-L2 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site to which you want to add the access interface; expand the entries for that site.

5 Right-click on L2 Access Interfaces and choose Create I-L2 Access Interface. The I-L2 Access Interface (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Description
- Administrative State
- MC Ring Node
- Tunnel Fault Notification

Tunnel Fault Notification is configurable on interfaces where the device has ports configured in access or hybrid mode with QinQ encapsulation.

If you are configuring a tunnel facility MEP, Tunnel Fault Notification must be set to Accept.

7 Choose a transit prefix policy for the interface, if required.

i Click on the Select button in the Transit Prefix Policy panel. The Select Transit Prefix Policy - VPLS I-L2 Access Interface form opens.

ii Select a transit prefix policy and click on the OK button.

8 Choose an SHG for the interface, if required.

i Click on the Select button in the Split Horizon Group panel. The Select Split Horizon Group Name - I-L2 Access Interface form opens.



Note — You must configure an SHG or residential SHG for a VPLS if you plan to create a spoke circuit from this VPLS site to a VLL or another VPLS.

ii Select an SHG and click on the OK button. The Select Split Horizon Group Name - I-L2 Access Interface form closes, and the I-L2 Access Interface (Create) form refreshes with the SHG name.

9 Click on the Port tab.

10 Click on the Select button to choose a port for the I-L2 access interface. The Select Terminating Port - VPLS I-L2 Access Interface form opens.



Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

11 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - VPLS I-L2 Access Interface form closes, and the VPLS I-L2 Access Interface (Create) form displays the port information.



Note — If you select an Ethernet Tunnel Endpoint, the Port form is refreshed and an Ethernet Tunnel tab is added.

12 Configure the parameters:

- Outer Encapsulation Value
- Inner Encapsulation Value



Caution — The creation of a SAP that uses the same port and encapsulation values as an existing inactive MSAP fails under the following conditions:

- If you try to use the 5620 SAM to create a SAP, the configuration fails and the 5620 SAM displays an error message.
- If you use a CLI to create a SAP in a service other than the service that contains the MSAP, the configuration succeeds but the MSAP is inactive until the regular SAP is deleted. Although the 5620 SAM displays the SAP and MSAP, the MSAP remains inactive and consumes resources.
- If you use a CLI to create a SAP in the service that contains the MSAP, the SAP creation fails.

Alcatel-Lucent recommends that you delete an inactive MSAP from the 5620 SAM if you need to create a regular SAP on the same port using the same encapsulation values. See Procedure 65-34 for more information about deleting MSAPs.

For an I-L2 access interface, only Null, dot1q, and QinQ encapsulations are supported. In the case of I-MPVLS L2-access interfaces, Null encapsulation is not supported. I-MPVLS L2-access interfaces with MSTP configured support QinQ. These ports must also be of Ethernet type PBB.

When the selected port uses dot1q encapsulation, you can enable the Auto-Assign ID parameter to have the Outer Encapsulation Value parameter automatically assigned. If you choose this, the system assigns the lowest unused encapsulation value.



Note — You can set the Auto-Assign ID parameter to be the default parameter for dot1q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter in the User Preferences form. Choose Application→ User Preferences from the main menu.

The Inner Encapsulation Value is configurable only when the port is an Ethernet with QinQ encapsulation.

If the port you have chosen is an Ethernet Tunnel Endpoint, you will be able to set the Outer Encapsulation Value to 8191. This automatically enables the Ethernet Tunnel Endpoint Control SAP parameter.

13 Configure the Ethernet Tunnel Endpoint Control SAP parameter, if required.



Note — Enabling the Ethernet Tunnel Endpoint Control SAP parameter creates the control L2 Access Interface (also known as a Control SAP). It also automatically sets the value of the Outer Encapsulation Value parameter to 8191.

If you are currently creating a same-fate SAP, the Ethernet Tunnel Endpoint Control SAP parameter must not be enabled.

14 Depending on the port that you have chosen, the Egress Multicast Group tab is configurable. Configure the EMG, if required.

i Click on the Egress Multicast Group tab. The Select Egress Multicast Group-I-L2 Access Interface form opens.

ii Select an EMG and click on the OK button. The Select Egress Multicast Group-I-L2 Access Interface form closes, and the Egress Multicast Group tab refreshes with the EMG name.



Note — The Egress Multicast Group-L2 Interface form lists only EMGs that have the same egress filter and encapsulation type as the interface.

15 If the selected port uses FR encapsulation, configure Frame Relay for the interface.

i Click on the Frame Relay tab.

ii Set the FRF-12 Mode parameter to Enabled.

iii Configure the parameters:

- FRF-12 End-To-End Fragment Threshold
- Scheduling Class
- Fragment Interleave

16 Assign ingress and egress QoS policies to the interface, if required.

i Click on the QoS tab.



Note — Items such as policies, schedulers, and filters can be applied later to multiple service components at once by selecting and right-clicking the components in the service navigation tree, choosing Properties, and configuring the parameters on the appropriate tab. This action opens a properties form in a new window for the component that was right-clicked. The navigation tree is not displayed in this new window.

ii Configure the Ingress Match QinQ Dot1P parameter.

The Ingress Match QinQ Dot1P parameter is configurable only when the encapsulation type of the port is dot1q or QinQ.

iii Click on the Select button in the Ingress Policy panel to choose an ingress QoS policy. The Select Ingress Policy - I-L2 Access Interface form opens.

iv Select an ingress QoS policy and click on the OK button. The Select Ingress Policy - I-L2 Access Interface form closes, and the I-L2 Access Interface (Create) form refreshes with the ingress QoS policy name.



Note — If you select an access ingress policy which has a forwarding class mapped to an ingress queue group, you must ensure that port that you are configuring for the VPLS L2 access interface has the access ingress queue group with the same name created on it.

See Procedure 16-1 in chapter 16 for more information about how to configure Ethernet ports. See chapter 42 for more information about queue group template policies.

v Click on the Ingress Queue Group Template Policy Select button in the Forwarding Plane Redirect panel to choose a policy. The Select Forwarding Plane Queue Group Instance form opens.

vi Choose a policy from the list and click on the OK button. The Select Forwarding Plane Queue Group Instance form closes. The VPLS L2 Access Interface (Create) form refreshes with the Ingress Queue Group Template Policy information displayed.

vii Configure the Instance ID parameter.

viii Configure the Egress Mark QinQ Top Bits Only parameter.

The Egress Mark QinQ Top Bits Only parameter is configurable only when the encapsulation type of the port is dot1q or QinQ.

ix Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - I-L2 Access Interface form opens.

x Select an egress QoS policy and click on the OK button. The Select Egress Policy - I-L2 Access Interface form closes, and the I-L2 Access Interface (Create) form refreshes with the egress QoS policy name.



Note — If you select an access egress policy which has a forwarding class mapped to an egress queue group, you must ensure that port that you are configuring for the VPLS L2 access interface has the access egress queue group with the same name created on it.

See Procedure 16-1 in chapter 16 for more information about how to configure Ethernet ports. See chapter 42 for more information about queue group template policies.

xi If the port you selected in step 11 is not an HSMDA port then go to step 17.

xii Configure the Packet Byte Offset (bytes) parameter, if required. Before you can configure the parameter, you must select the associated Override check box.

xiii Click on the Select button in the Egress HSMDA Override panel to choose a WRR policy. The Select WRR Policy form opens.

xiv Choose a WRR policy and click on the OK button. The Select WRR Policy form closes and the VPLS L2 Access Interface (Create) form reappears with the WRR policy information displayed.

xv Click on the Select button in the Egress HSMDA Override panel to choose an HSMDA egress secondary shaper policy. The Select Secondary Shaper form opens.

xvi Choose a secondary shaper and click on the OK button. The Select Secondary Shaper form closes and the VPLS L2 Access Interface (Create) form reappears with the secondary shaper information displayed.

xvii Configure the parameters:

- Use Shared Queue
- Use Multipoint Shared Queue

17 Click on the Schedulers tab to configure scheduling; otherwise, go to step 19.



Note — The Schedulers tab is configurable only when a port is assigned to the interface.

18 Perform one of the following.

a Specify that an aggregation scheduler policy is not applied to the interface.

i Set the Aggregation parameter to off.



Note — The Aggregation parameter is not configurable if the port you selected in step 11 is an HSMDA port.

ii Configure the parameters:

- Aggregate Rate Limit (kbps)
- Frame-Based Accounting



Note 1 — The Aggregate Rate Limit (kbps) and Frame-Based Accounting parameters are configurable only when there is no scheduler specified in the Egress Scheduler panel.

Note 2 — The Frame-Based Accounting parameter is not configurable if the port you selected in step 11 is an HSMDA port.

Note 3 — You cannot specify an egress scheduler when the Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

iii Click on the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - I-L2 Access Interface form opens.

iv Select an ingress scheduler and click on the OK button. The Select Ingress Scheduler - I-L2 Access Interface form closes, and the I-L2 Access Interface (Create) form refreshes with the ingress scheduler information displayed.

v Click on the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Policer Control Policy form opens.

vi Choose a policer control policy and click on the OK button. The Select Policer Control Policy form closes and the VPLS I-L2 Access Interface (Create) form reappears with the ingress policer control policy information displayed.

vii If the port you selected in step 11 is an HSMDA port, go to step 19.

viii Click on the Select button in the Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - I-L2 Access Interface form opens.

ix Select an egress scheduler and click on the OK button. The Select Egress Scheduler - I-L2 Access Interface form closes, and the I-L2 Access Interface (Create) form refreshes with the egress scheduler information displayed.

x Click on the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Policer Control Policy form opens.

xi Choose a policer control policy and click on the OK button. The Select Policer Control Policy form closes and the VPLS I-L2 Access Interface (Create) form reappears with the egress policer control policy information displayed.

xii Go to step 19.

b Specify that an access scheduler policy is applied to the interface.



Note — You cannot specify an access scheduler policy if the port you selected in step 11 is an HSMDA port. Go to step 19.

i Set the Aggregation parameter to on.

ii Click on the Select button in the Aggregation Scheduler panel to choose an aggregation scheduler. The Select Aggregation Scheduler - I-L2 Access Interface form opens.

iii Select an aggregation scheduler and click on the OK button. The Select Aggregation Scheduler - I-L2 Access Interface form closes, and the I-L2 Access Interface (Create) form refreshes with the aggregation scheduler information displayed.

19 Assign ingress and egress ACL filters to the interface, if required.

i Click on the ACL tab.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - I-L2 Access Interface form opens.

iii Select an ingress ACL filter and click on the OK button. The Select Ingress Filter - I-L2 Access Interface form closes, and the I-L2 Access Interface (Create) form refreshes with the ingress ACL filter name.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - I-L2 Access Interface form opens.

v Select an egress ACL filter and click on the OK button. The Select Egress Filter - I-L2 Access Interface form closes, and the I-L2 Access Interface (Create) form refreshes with the egress ACL filter name.

vi Click on the Select button in the IPv6 Ingress Filter panel to choose an IPv6 ingress ACL filter. The Select IPv6 Ingress Filter - I-L2 Access Interface form opens.

vii Select an IPv6 ingress ACL filter and click on the OK button. The Select IPv6 Ingress Filter - I-L2 Access Interface form closes and the I-L2 Access Interface (Create) form reappears with the IPv6 ingress ACL filter information displayed.

viii Click on the Select button in the IPv6 Egress Filter panel to choose an IPv6 egress ACL filter. The Select IPv6 Egress Filter - I-L2 Access Interface form opens.

ix Select an IPv6 egress ACL filter and click on the OK button. The Select IPv6 Egress Filter - I-L2 Access Interface form closes and the I-L2 Access Interface (Create) form reappears with the IPv6 egress ACL filter information displayed.

20 Assign an accounting policy to the interface, if required.

i Click on the Accounting tab.

ii Configure the Collect Accounting Statistics and Ingress Counter Type parameters.

iii Click on the Select button to choose an accounting policy. The Select Accounting Policy - I-L2 Access Interface form opens.

iv Select an accounting policy and click on the OK button. The Select Accounting Policy - I-L2 Access Interface form closes, and the I-L2 Access Interface (Create) form refreshes with the accounting policy name.

21 Configure BPDU Termination, STP, and FIB parameters for the interface, if required.

i Click on the Forwarding Control tab. Depending on the device being configured, the BPDU Termination tab is displayed. Otherwise, go to step iii.

ii Configure the parameters:

- L2 Protocol Termination
  When the L2 Protocol Termination parameter is set to Enabled, a list of L2PT protocols is displayed. Select all that are required.
- BPDU Translation
- Force L2PT on Managed L2 Access Interface
  The Force L2PT on Managed L2 Access Interface parameter is only available for MVPLS I-L2 access interfaces. When the Force L2PT on Managed L2 Access Interface parameter is set to Enabled, a list of L2PT protocols is displayed. Select all that are required.

iii Click on the STP tab.

iv Configure the parameters:

- Path Cost
- Port Number
- Priority
- Edge Port
- Edge Capability Detection
- Link Type
- Root Guard
- Administrative State

v Click on the FIB tab.

vi Configure the parameters:

- Aging Enabled
- Learning Enabled
- Maximum Entries
- Limit Mac Move
- Limit Mac Move Level
- Discard Unknown Source
- Restrict Protected Source
- Restrict Protected Source Action
- Restrict Unprotected Destination

vii If you are creating an MVPLS to run MSTP, the MST Instances tab is configurable. Otherwise, go to step 22.

viii Click on the MST Instances tab to edit a SAP MST instance.

ix Select an MST instance and click on the Properties button.

x The I-L2 Access Interface MST Instance (Edit) form opens. Configure the parameters:

- Path Cost
- Priority

xi Click on the OK button to close the I-L2 Access Interface MST Instance (Edit) form. A dialog box appears.

xii Click on the OK button. The I-L2 Access Interface (Create) form refreshes with the new MST instance.

22 Assign a DoS protection policy or DDoS protection policy to the interface, if required.



Note — A default DoS protection policy is automatically assigned to the interface.

i Click on the Security tab.

ii Click on the Select button in the NE DoS Protection panel and select a DoS protection policy from the Select NE DoS Protection - I-L2 Access Interface form.

iii Click on the Select button next to the NE DDoS Protection Policy panel and select a DDoS protection policy from the Select NE DDoS Protection Policy - I-L2 Access Interface form.

iv Configure the MAC Monitoring parameter.

23 Configure an Ethernet tunnel.



Note — You can only configure Ethernet tunnel SAP path parameters if you are creating a same-fate SAP.

i Click on the Ethernet Tunnel tab.

ii If you are configuring a fate-sharing Ethernet Tunnel Endpoint SAP (also referred to as same-fate SAP) then go to step iii. Otherwise, go to step 24.

iii Click on the Create button. The Ethernet Tunnel (Create) form opens.

iv Configure the parameters:

- Path ID
- Tag (Outer Encapsulation Value)
- Tag (Inner Encapsulation Value)

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The L2 Access Interface (Create) form refreshes with the Ethernet Tunnel entry.

24 Configure a redundant VLAN range, if required.



Note — If an MVPLS site has SAPs that manage traffic on the associated VPLS SAPs, you must define a redundant VLAN range during SAP creation. The redundant VLAN range defines the range of VC IDs for VPLS SAPs that the MVPLS manages.

i Click on the Redundancy tab.

ii Click on the Create button. The RedundantVlanRange (Create) form opens.

iii Configure the parameters:

- Min VLAN ID
- Max VLAN ID

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The I-L2 Access Interface (Create) form refreshes with the redundant VLAN range entry.

25 Configure IGMP snooping for the interface, if required.

i Click on the IGMP Snooping tab. The General tab is displayed.

ii Configure the parameters:

- Import Policy
- Fast Leave
- Multicast Router Attached
- Send Queries
- General Query Interval (seconds)
- Maximum Response Interval (seconds)
- Robust count
- IGMP Version
- Last Member Query Interval (tenths of seconds)
- Maximum Number of Groups
- Maximum Number of Sources per Group
- Maximum Number of Group Sources per Group

The General Query Interval (seconds), Maximum Response Interval (seconds), Robust count, and IGMP Version parameters are configurable when the Send Queries parameter is enabled.

iii Click on the Static Mcast Group tab to configure a static multicast group, if required. Otherwise, go to step 26.

iv Click on the Create button. The Access Interface Igmp Snooping Mcast Group Display (Create) form opens.

v Configure the parameters:

- Group Address
- Source Address

vi Click on the Apply button if you want to create additional entries. A dialog box appears.

vii Click on the OK button.

viii Repeat steps iv to vii to create an additional entry, if required.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Static Mcast Group tab refreshes with the new multicast group entries.

26 Configure anti-spoofing filters for the interface, if required.

i Click on the Anti-Spoofing tab.

ii Configure the MAC Pinning parameter.

27 Specify the queue overrides.

i Click on the Override Policy Items tab.



Note — The Override Policy Items tab contains a number of tabs. However, the tabs that are displayed depend on the port type that you have chosen for this interface.

- If you configured a non-HSMDA port, then the Access Ingress Queues, Access Egress Queues, Ingress Policer, and Egress Policer tabs are active.
- If you configured an HSMDA port, then the Access Ingress Queues, Access Egress HSMDA Queues and Ingress Policer tabs are active.

ii See Procedure 43-42 for information about setting queue overrides.

28 Associate a MEP with the I-L2 Access interface, if required.

i Click on the ETH-CFM tab.

ii Configure the Tunnel Fault Notification parameter.

iii Click on the Create button in the Virtual MEP panel. The MEP (Create) form opens with the General tab displayed.

iv Click on the Select button. The Select Maintenance Entity Group form opens.

v Select an entry and click on the OK button. The Select Maintenance Entity Group form closes.

vi Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- Description
- MAC Address
- CCM Enabled
- Priority Level for CCM
- Fault Propagation
- CCM Padding Packet Size (Bytes)
- Low-priority Defect



Note — The CCM Padding Packet Size (Bytes) parameter cannot be configured when the CCM interval parameter is set to 10 ms or 100 ms.

vii As required, configure the Test Generation Options parameters:

- Role
- Use as Test Source
- Use as Test Target



Note — The Role, Use as Test Source, and Use as Test Target parameters are configurable only when you set the Direction parameter to Up.

viii If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab. Otherwise, go to step xii.

ix Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

x Click on the AIS tab.

xi Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

xii Click on the OK button. The MEP (Create) form closes.

29 Assign an ANCP policy to the interface, if required.

- **i** Click on the ANCP Static Map tab.
- **ii** Click on the Create button. The ANCP Static Map (Create) form opens.
- **iii** Configure the ANCP String parameter.
- **iv** Click on the Select button to choose an ANCP Policy. The Select ANCP Policy - ANCP Static Map form opens.
- **v** Select an ANCP policy and click on the OK button. The Select ANCP Policy - ANCP Static Map form closes and the ANCP Static Map form reappears with the ANCP policy information displayed.
- **vi** Click on the OK button. The ANCP Static Map form closes.

30 Click on the OK button. The I-L2 Access Interface (Create) form closes and a dialog box appears.

31 Click on the Yes button. The VPLS Service (Edit) form reappears.

32 Repeat steps 4 to 31 for each additional I-L2 access interface that you want to create.

33 Click on the OK button. A dialog box appears.

34 Click on the Yes button. The VPLS Service (Edit) form closes.

35 Close the Manage Services form.

Procedure 68-71 To configure a GNE site on a VPLS service

Use this procedure to add a GNE site and GNE service interfaces to an existing VPLS service.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS service and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the component tree, right-click on VPLS Service and choose Create GNE Site. The Select Network Elements - VPLS Service form opens with a list of available sites.

5 Choose a site and click on the OK button. The GNE Site (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Name
- Description

7 Click on the Apply button.

8 To configure an interface for the GNE site, perform the following steps:

i Click on the GNE Service Interfaces tab and then click on the Create button. The GNE Service Interface (Create) form opens with the general tab displayed.

ii Configure the parameters:

- Name
- Description
- Type

iii Click on the Ports tab and then click on the Select button beside the Interface Index field. The Select Generic NE Interface form appears.

iv Select an interface from the list and click on the OK button. The GNE Service Interface (Create) form reappears with the interface information displayed.

v Configure the parameters:

- Encapsulation Type
- Outer Encapsulation Value
- Inner Encapsulation Value

vi Click on the OK button. The GNE Site (Create) form reappears with the interface information displayed in the service component tree.

9 Click on the Scripts tab to attach or execute configuration scripts on the GNE site.

The Scripts tab displays the script instances and versions that are applied to the device. See “Creating and executing scripts” in the *5620 SAM Scripts and Templates Developer Guide* for more information.

10 Click on the OK button. The VPLS Service (Edit) form reappears with the new information displayed in the service component tree.

11 Click on the OK button. The VPLS Service (Edit) form closes.

You can use the topology maps to view the service. See chapter 6 for more information about service topology maps.

Procedure 68-72 To force a switchover to a redundant spoke SDP binding

This procedure can only be performed on a VPLS that has been configured with endpoints that are associated redundant spoke SDP bindings.

1 Choose Manage→Service→Services from the 5620 SAM main menu.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Select the required VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site where you want to perform the switchover; expand the entries for that site.

5 Right-click on the redundant spoke SDP binding under an endpoint for the site that you want to perform the switchover for.

6 Select Force Switchover from the popup menu.

7 You can clear the switchover at a later time by performing steps 1 to 5 again and then select the Clear Forced Switchover item from the popup menu.



Note — You must clear a manually forced switchover by using the Clear Forced Switchover button when the active spoke SDP binding is restored. The 5620 SAM cannot automatically switch to another active spoke SDP binding if this is not done.

8 Click on the OK button to close the Spoke SDP Binding (Edit) form.

9 Click on the OK button to close the VPLS Service (Edit) form.

Procedure 68-73 To run a VPLS service OAM validation test

An OAM validator test suite must be created for the tested entity. See chapter 77 for more information about how to create a validator test suite.



Note 1 — As an alternative, you can also run an OAM validation test on the service by performing a One Time Validation. This is a mostly automated procedure and is described in Procedure 77-9.

Note 2 — OAM validation tests are not supported for HVPLS.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears at the bottom of the Manage Services form.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 Click on the Validate button. If the Validate button is not visible, click on the More Actions button and choose Validate. If an OAM validator test suite is not associated to the service, a dialog box appears. Perform the following steps:

   i Click on the OK button to associate the service with an existing OAM validator test suite. The Choose Validator Test Suite form appears.

   ii Configure the filter criteria. A list of OAM validator test suites appears.

   iii Select an OAM validator test suite and click on the OK button. The Choose Validator Test Suite form closes.

5 View the State Cause indicators. When the validation test fails, a check mark appears beside the OAM Validation Failed indicator.

6 Click on the Tests tab. The Test Suite tab is displayed.

7 Click on the Tested Entity Result tab.

8 Choose an entry and click on the Properties button. The Tested Entity Result (Edit) form opens with the General tab displayed.

9 Click on the Results tab to display the validation test results.

10 If you need to compare two test results from the same type of test, choose the two test results and click on the Compare button; the Difference form opens. Otherwise go to step 13.

11 Compare the test results.

12 Close the Difference form.

13 Close the Tested Entity Result form.

14 Close the VPLS Service (Edit) form.

15 Close the Manage Services form.

Procedure 68-74 To add or modify FIB entries associated with a VPLS

1 Choose Manage→Service→FIB Entries from the 5620 SAM main menu.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 Click on the Forwarding Control tab.

5 Click on the FIB Entries tab.

6 Click on the Search button. A list of FIB entries appears.

7 Add or modify FIB entries as required.

a To add a FIB entry:

i Click on the Create button. The FIB Entry (Create) form opens.

ii Configure the parameters:

- MAC Address
- Auto Complete

iii Choose an interface, service circuit, or endpoint from the list on the L2 Interfaces, Service Circuits, or Endpoints tab.

iv Click on the OK button. The FIB Entry (Create) form closes, and the FIB Entries form refreshes with the new FIB entry.

b To modify FIB entries:

i Choose a FIB entry from the list and click on the Properties button. The FIB Entry (Edit) form opens.

ii Configure the parameters and view the information as required.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button to close the VPLS Service (Edit) form.

Procedure 68-75 To list FIB entries associated with a VPLS

1 Choose Manage→Service→FIB Entries from the 5620 SAM main menu.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 Click on the Sites tab.

5 Click on the VPLS, B-VPLS, or I-VPLS tabs, if required.

6 Select the site can click on the Properties button. The VPLS Site (Edit) form opens with the General tab displayed.

7 Click on the Forwarding Control tab.

8 Click on the FIB Entries tab.

9 Click on the Resync button for the FIB entries on the right side of the form. The Resync button on the bottom of the form is for re synchronizing the entire VPLS site.

10 Click on the Find button. A list of FIB entries appears.

Procedure 68-76 To view the service topology associated with a VPLS service

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears at the bottom of the Manage Services form.

3 Choose a VPLS and click on the Topology View button. The Service Topology map opens.

See chapter 6 for more information about service topology views.



Note — In the VPLS topology map view, a redundant spoke SDP binding under an endpoint displays differing colors, depending on whether it is in the active or backup state. Backup spoke SDP bindings are shown in purple.

4 Close the Service Topology form.

5 Close the Manage Services form.

Procedure 68-77 To view the VPLS service operational status

The Aggregated Operational State and State Cause indicators on the General tab of the service management form display information about service faults.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears at the bottom of the Manage Services form.

3 Select a service and click on the Properties button. The VPLS Service (Edit) form opens.

4 View the Aggregated Operational State and State Cause indicators. When the Aggregated Operational State is Down or Partially Down, a check mark beside the appropriate State Cause indicator identifies the type of associated service fault.

5 Click on the appropriate tab to view or edit an object that is identified as faulty by a State Cause indicator.

6 Click on the Faults tab to view the alarms for the object. The Object Alarms tab is displayed.

7 Click on the Aggregated Alarms tab to view the aggregated alarms for the object, if required.

8 Click on the Tests tab if the OAM Validation Failed indicator is enabled. You can view the OAM validation test suite results by clicking on the Tested Entity Result tab.



Note 1 — You can run the OAM Validation test suite for this service from this form by clicking on the Validate button. If the Validate button is not visible, click on the More Actions button and choose Validate.

Note 2 — As an alternative, you can also run an OAM validation test on the service by performing a One Time Validation. This is a mostly automated procedure and is described in Procedure 77-9.

9 Close the VPLS Service (Edit) form.

10 Close the Manage Services form.

Procedure 68-78 To view IGMP snooping queriers

1 Choose Manage→Service→Services from the 5620 SAM main menu.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on a site. The Site (Edit) form opens with the General tab displayed.

5 Click on the Multicast tab.

6 Click on the IGMP Snooping tab. The General tab is displayed.

7 Click on the MRouters tab. The MRouters table displays a list of IGMP snooping queriers and their properties.

8 Click on the Refresh button to view periodic updates to the Mrouters table.

9 Close the Site (Edit) form.

10 Close the VPLS Service (Edit) form.

Procedure 68-79 To view MLD snooping queriers

1 Choose Manage→Service→Services from the 5620 SAM main menu.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on a site. The Site (Edit) form opens with the General tab displayed.

5 Click on the Multicast tab.

6 Click on the MLD Snooping tab. The General tab is displayed.

7 Click on the MRouters tab. The MRouters table displays a list of MLD snooping queriers and their properties.

8 Click on the Refresh button to view periodic updates to the Mrouters table.

9 Close the Site (Edit) form.

10 Close the VPLS Service (Edit) form.

Procedure 68-80 To modify a VPLS



Caution — Modifying parameters can be service-affecting.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

The following tabs contain parameter information for the service:

- General tab—displays the general service properties
- MVR tab—displays multicast package policy information for the service
- Bandwidth tab — displays service tunnel bandwidth booking information for the service.
- Tests tab—allows the creation and execution of service-specific diagnostic tests
- Forwarding Control tab—lists the FIB and STP instances
- Sites tab—lists the sites that belong to the service
- L2 Access Interfaces tab—lists the L2 access interfaces that belong to the service
- L2 Management Interfaces tab—lists the L2 management interfaces that belong to the service
- Mesh SDP Bindings tab—displays the mesh SDP bindings that belong to the service
- Spoke SDP Bindings tab—displays the spoke SDP bindings that belong to the service, including active and backup SDP bindings associated with endpoints.
- Endpoints tab—displays the endpoints associated with the service
- Template tab—displays the template used to create the service, if applicable
- Faults tab—displays the faults associated with the service



Note — Users with the administrator scope of command role can click on the Select button on the Template tab to associate a service template with the service object, if required.

4 Navigate to related components for the service using the navigation tree, as required.

Certain service components have related objects that can be easily examined using the navigation tree. For such objects, right-clicking them in the navigation tree offers a “Navigate to...” option in the contextual menu. If you select this option, the properties form for the related object is displayed. This can be very convenient, especially for complex services containing many sites and components.

The VPLS components for which you can navigate to such related objects include:

- I-Sites: you can navigate to the associated B-VPLS or B-(M)VPLS
- L2 Access Interfaces: you can navigate to the opposite SAP in a VLAN Uplink configuration
- Redundant L2 Access Interfaces: you can navigate to the opposite SAP.
- Mesh SDP Bindings: you can navigate to the opposite (return) mesh SDP
- Spoke SDP Bindings: you can navigate to the opposite (return) spoke SDP

5 Modify the components and parameters for the service, as required.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The VPLS Service (Edit) form closes, and the Manage Services form reappears.

8 Close the Manage Services form.

Procedure 68-81 To modify a VLPS using the topology view

The topology view for a service provides a graphical representation of the various components and their interconnections. You can also use this view to add, modify, or just navigate to service components. This provides an alternative approach to performing these functions from the navigation tree view.

Working from the topology view can expedite the creation of the components, since many of the fields you would ordinarily have to set in the configuration forms will be automatically populated using this approach. The configuration forms can also be accessed directly at any time from this view by right-clicking a component. This allows quick access to conduct more detailed component configuration.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears at the bottom of the Manage Services form.

3 Choose a VPLS and click on the Topology View button. The Service Topology map opens.

The remainder of this procedure contains a number of sub-procedures describing the various components that can be created and modified from the topology view. These include:

- Creating a new site. Go to step 4.
- Creating site components. Go to step 10.
- Creating SDP bindings. Go to step 23.

Adding a new site

4 Right-click on any blank space in the service topology map. A contextual menu is displayed. You can choose to create one of the following:

- VPLS Site
- VPLS B-Site
- VPLS I-Site

5 Select the required option. The Select Network Elements form appears.

6 Select one or more sites to add to the service and click OK. The VPLS Site (Create), VPLS I-Site (Create), or VPLS B-Site (Create) form is displayed, depending on your menu item selection. If you selected more than one site, the VPLS Site (Multiple Instances) (Create), VPLS I-Site (Multiple Instances) (Create), or VPLS B-Site (Multiple Instances) (Create) form is displayed, depending on your menu item selection.

7 Click on the OK button. The VPLS Site (Create) (or VPLS Site (Multiple Instances) (Create)) form closes and the new site (or sites) is displayed on the map.

8 If you want to perform detailed configuration of site properties for the new site, right-click on the site icon and select Properties from the contextual menu. The VPLS Site (Edit) form opens. Refer to Procedure 68-1 for detailed site configuration information.

9 Return to step 3 for a list of other functions you can perform from the topology view or go to step 53 to finish.

Creating site components

10 Right-click on any site icon in the service topology map. A contextual menu is displayed. You can choose to create one of the following:

- VPLS L2 Access Interface (this choice will actually display as either a regular L2 Access Interface, or a B-L2 or I-L2 variant, depending on the site you select). Go to step 11.
- VPLS L2 Management Interface. Go to step 15.
- VPLS Endpoint. Go to step 19.

11 If you choose to create a VPLS L2 Access Interface, then the VPLS L2 Access Interface (Create) form is displayed. If the selected site is a B-Site or I-Site, then the B-L2 or I-L2 Access Interface (Create) form is displayed accordingly.

12 Click on the Port tab and assign a port to the interface.

Refer to Procedure 68-24 (or Procedure 68-66 or 68-70 for B-L2 or I-L2 Access Interfaces respectively) for detailed information on further configuring the interface, if required.

13 Click on the OK button. The VPLS L2 Access Interface (Create) form closes.

14 Go to step 22.

15 If you choose to create a VPLS L2 Management Interface, then the VPLS L2 Management Interface (Create) form is displayed.

16 Click on the Port tab and assign a port to the interface.

Refer to Procedure 68-24 for detailed information on further configuring the interface, if required.

17 Click on the OK button. The VPLS L2 Management Interface (Create) form closes.

18 Go to step 22.

19 If you choose to create a VPLS Endpoint, then the Endpoint (Create) form is displayed.

20 Configure the Name parameter for the endpoint.

Refer to Procedure 68-1 (or 68-60 for B-Sites) for detailed information on further configuring the endpoint, if required.

21 Click on the OK button. The Endpoint (Create) form closes and the new endpoint is displayed in the topology view.

22 Return to step 3 for a list of other functions you can perform from the topology view or go to step 53 to finish.

Creating SDP bindings

23 Select the sites you want to connect in the service topology map and right-click on any one of them. A contextual menu is displayed.



Note 1 — If you intend to create either a spoke or a mesh binding between two sites, the order in which you select them is important. The first site you select will become the source site and the second site will become the destination site. Therefore, it is not recommended that you do a marquee-select in the topology view, since you will not be sure of this hierarchy. Instead, select the sites individually, and hold down the Shift or Ctrl key after your first selection.

Note 2 — If you intend to create a full mesh between sites, then the order in which you select the sites is not important.

Note 3 — If you intend to add a service site to an existing mesh of sites, then the first site you select must be the one that is not currently a part of the mesh. The second site you select can be any member of the existing mesh.

24 Select Connect from the contextual menu. Depending on the sites you selected, one or more of the following options are available:

- Create Spoke SDP Binding. Go to Step 25.
- Create Mesh SDP Binding. Go to Step 32.
- Create Full Mesh. Go to Step 39.
- Add To Existing Mesh. Go to Step 46.

25 If you choose the Create Spoke SDP Binding option, then the Spoke SDP Binding (Create) form is displayed.



Note 1 — For this function, it is assumed that you clicked on the source site first and then held down the Shift or Ctrl key while right-clicking on the destination site to display the contextual menu.

Note 2 — You can also create a spoke SDP binding between a site icon and an endpoint icon, or between two endpoint icons in the topology view. Appropriate endpoints must first exist or be created to enable this.

26 Enable the Auto-Select Transport Tunnel parameter.

27 You can manually configure other parameters here if required, or just click on the OK button. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Spoke SDP Binding (Create) form closes and the new binding between the two sites is displayed in the topology view. Refer to Procedure 68-44 for more detailed information on creating and configuring spoke SDP bindings, if required.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. Refer to Chapter 27 for information on how to create the required tunnel. Once the tunnel is created, you can repeat this sub-procedure.

28 Assuming that the spoke SDP binding was successfully created in step 27, select the same two sites again in the topology view, although this time do so in the opposite order that you originally selected them. This will allow you to create a spoke binding for the return tunnel.

29 Right-click on the second site you selected and choose the Create Spoke SDP Binding ... option from the contextual menu. The Spoke SDP Binding (Create) form is displayed.

30 You can manually configure other parameters here if required, or just click on the OK button. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Spoke SDP Binding (Create) form closes and the new return binding between the two sites is displayed in the topology view.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. Refer to Chapter 27 for information on how to create the required tunnel. Once the tunnel is created, you can repeat this sub-procedure.

31 Return to step 3 for a list of other functions you can perform from the topology view or go to step 53 to finish.

32 If you choose the Create Mesh SDP Binding option, then the Mesh SDP Binding (Create) form is displayed.



Note — For this function, it is assumed that you clicked on the source site first and then held down the Shift or Ctrl key while right-clicking on the destination site to display the contextual menu.

33 Enable the Auto-Select Transport Tunnel parameter.

34 You can manually configure other parameters here if required, or just click on the OK button. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Mesh SDP Binding (Create) form closes and the new binding between the two sites is displayed in the topology view. Refer to Procedure 68-43 for more detailed information on creating and configuring mesh bindings, if required.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. Refer to Chapter 27 for information on how to create the required tunnel. Once the tunnel is created, you can repeat this sub-procedure.

35 Assuming that the mesh SDP binding was successfully created in step 34, select the same two sites again in the topology view, although this time do so in the opposite order that you originally selected them. This will allow you to create a mesh binding for the return tunnel.

36 Right-click on the second site you selected and choose the Create Mesh SDP Binding ... option from the contextual menu. The Mesh SDP Binding (Create) form is displayed.

37 You can manually configure other parameters here if required, or just click on the OK button. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Mesh SDP Binding (Create) form closes and the new return binding between the two sites is displayed in the topology view.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. Refer to Chapter 27 for information on how to create the required tunnel. Once the tunnel is created, you can repeat this sub-procedure.

38 Return to step 3 for a list of other functions you can perform from the topology view or go to step 53 to finish.

39 If you choose the Create Full Mesh option, the Complete Vpls Mesh for Service Component form is displayed.

40 Configure the Transport Type parameter.

41 Click on the Select button to display the Tunnel Selection Profiles form, if required.

42 Click on the Search button to display a list of available Tunnel Selection Profiles.

43 Click on the desired profile entry and click OK. The Tunnel Selection Profiles form closes and your selection is displayed in the Complete Vpls Mesh for Service Component form.

44 Click on the OK button to accept your selection and close the Complete Vpls Mesh for Service Component form. One of the following will result:

- If available transport tunnels exist between the selected sites, then the new mesh bindings between the sites are created and displayed in the topology view. Refer to Procedure 68-43 for more detailed information on creating and configuring mesh bindings, if required.
- If available transport tunnels do not exist between all the sites, then the new bindings that can be created are displayed, and an error message is also displayed informing you that the full mesh could not be completed. Refer to Chapter 27 for information on how to create the required tunnels. Once the tunnels are created, you can repeat this sub-procedure.

45 Return to step 3 for a list of other functions you can perform from the topology view or go to step 53 to finish.

46 If you choose the Add To Existing Mesh option, the Complete Vpls Mesh for Service Component form is displayed.

47 Configure the Transport Type parameter.

48 Click on the Select button to display the Tunnel Selection Profiles form, if required.

49 Click on the Search button to display a list of available Tunnel Selection Profiles.

50 Click on the desired profile entry and click OK. The Tunnel Selection Profiles form closes and your selection is displayed in the Complete Vpls Mesh for Service Component form.

51 Click on the OK button to accept your selection and close the Complete Vpls Mesh for Service Component form. One of the following will result:

- If available transport tunnels exist between the selected sites, then the new mesh bindings between the sites are created and displayed in the topology view. Refer to Procedure 68-43 for more detailed information on creating and configuring mesh bindings, if required.
- If available transport tunnels do not exist between the selected sites, then an error message is displayed to that affect. Refer to Chapter 27 for information on how to create the required tunnels. Once the tunnels are created, you can repeat this sub-procedure.

52 Return to step 3 for a list of other functions you can perform from the topology view or go to step 53 to finish.

53 Close the Service Topology form.

54 Close the Manage Services form.

Procedure 68-82 To delete a VPLS



Warning — Deleting a service may result in a service disruption for customers. Consider the implication of deleting the service before proceeding.



Note — A VPLS cannot be deleted if the L2 access interface has MSAPs that are in an active state. See chapter 65 for more information about MSAPs.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 As required, configure the filter criteria to locate the service or range of services to be deleted. Click on the Search button. A list of services appears at the bottom of the Manage Services form.

3 Choose a service or a range of services from the list.

4 Click on the Delete button. A warning form appears. This form is dynamic based on the priority of the service. Perform one of the following:

   a For services with a low priority, go to Step 5.

   b For services with a medium priority, configure the "Enter the highest priority of the service being deleted" text field by typing: Medium. Go to Step 5.

   c For services with a high priority, configure the "Enter the highest priority of the service being deleted" text field by typing: High. Go to step 5.

5 For all services, regardless of the priority configuration, acknowledge the check box that prompts you to confirm that you understand the implications of deleting the service.



Note — If you select multiple services with different priorities, you must enter the highest priority level of selected services before you can delete the services.

6 Click on the Yes button to confirm the action. The service is deleted and removed from the list.

7 Click on the Close button to close the Manage Services form.

69 — Mirror service management

69.1 Mirror service overview *69-2*

69.2 Sample mirror service configuration *69-4*

69.3 Workflow to create a mirror service *69-5*

69.4 Mirror service procedures *69-7*

69.1 Mirror service overview

The 5620 SAM GUI implementation of service mirroring provides mirroring of service traffic packets from any service type.



Caution — Service mirroring can affect performance across the network and in the source and destination devices, so must be planned accordingly.

In a mirror service, packets from one or more sources are forwarded to their normal destinations and a copy of the entire packet, or a specified portion of the packet, is sent to the mirror destination. The mirrored packet can be viewed using a packet-decoding device, typically called a sniffer, that is attached to the destination port. The 5620 SAM does not limit the number of destination and source sites added under a mirror service. The mirrored packets are transported unidirectionally through the core network using IP or MPLS tunneling.

With pseudo-wire redundancy support, an ICB can be enabled in the mirror service spoke and remote source, which can provide bidirectional service that enables support for active and standby PE redundancy. An endpoint can be used to group the redundant objects, which may be of mirror SDP bindings or SDP and SAP. In the mirror map view, the color for the active and backup states of the redundant mirror SDP differ.

Service mirroring can be used to do the following:

- Troubleshoot problems with customer packet delivery and content.
- Help service providers meet regulations by providing itemized call records and wiretaps, as authorized by investigative authorities.
- Simplify the complex traffic-analysis networks that are often implemented as overlays to the customer-facing network.

The 5620 SAM supports end-to-end mirror service configuration using the following methods:

- Tabbed configuration forms with an embedded navigation tree. The navigation tree provides a logical view of the service and acts as a configuration interface.
- Preconfigured template. A user who has the Administrator scope of command role, or the Mirror Service Management and Template Script Management roles, can create a mirror service template.
- The Lawful Interception Management scope of command role allows an LI user to view and configure LI sources on existing mirror services. Information that is mirrored is hidden from all users who do not have LI user privileges. See chapter 28 for more information about configuring a LI user.



Note — Viewing or retrieving LI user activity records requires a user account with an assigned Lawful Interception Management scope of command role. The scope is restricted to the records of users in the same LI user group.

The mirror service operational status is aggregated based on the status of each site.

- Aggregate status is down if all destination sites are down.
- Aggregate status is up if one of the redundant destination site is up.
- Aggregate status is down if all source sites are down.
- Aggregate status is up if one of the redundant source sites is up.
- Aggregate status is unknown if no sites are added to the service.

Consider the following before you implement a mirror service:

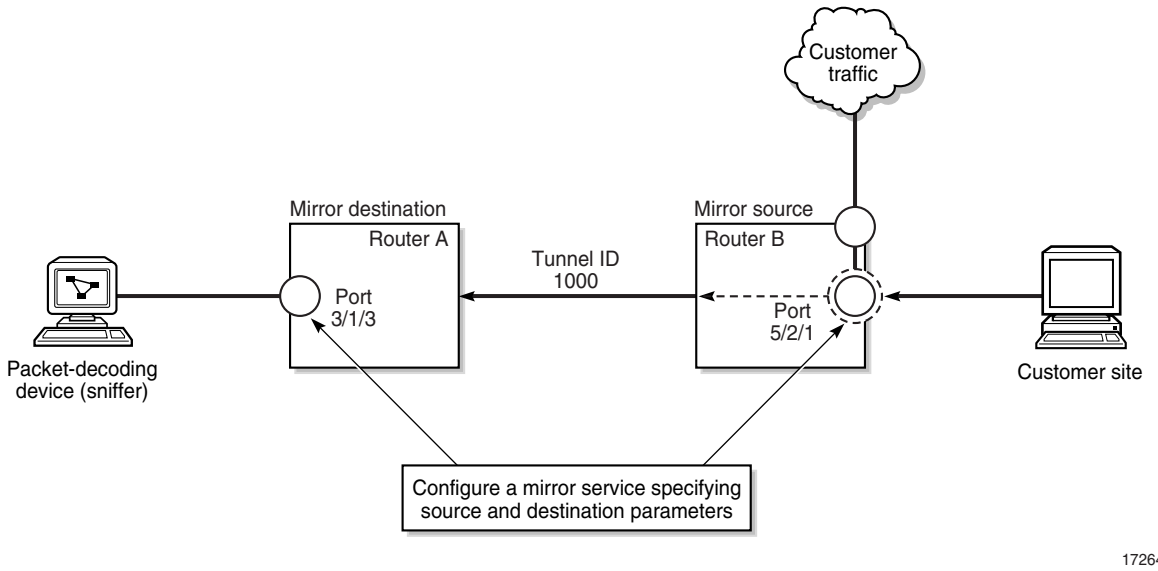
- You must be assigned the administrator or mirror service management scope of command role to create or modify a mirror service, or to view any mirror-related objects in the 5620 SAM.
- The default customer is automatically associated with a mirror service. You cannot associate a different customer with a mirror service.
- You can only configure one endpoint per mirror site.
- You can configure the endpoint in the destination site with SAP and SDP with ICB.
- An endpoint cannot have more than one SAP.
- You can create a mirror SDP under the endpoint in the destination site.
- You can create up to four mirror SDPs under the endpoint in the source site. One mirror SDP must have ICB. Alternatively, you can create one mirror SDP under the source site.
- When the mirror SDP binding is under an endpoint, the STP cannot be enabled on the spoke.
- Mirror sites with valid SAPs are considered as destination sites during discovery.
- You can configure a site as a destination without a SAP in the mirror service. During re-synchronization, the site type remains destination.
- Auto-SDP creation is restricted to one destination.
- You can change the redundancy setting of a mirror SDP binding by deleting and adding the mirror SDP binding on an endpoint.
- You cannot delete an MC-LAG SAP if an ICB is on the same endpoint.
- You cannot have a SAP with a non-ICB mirror spoke on the same endpoint.
- The destination of a mirror service must be an L2 SAP.
- You can mirror the ingress or egress traffic on SAPs and ports.
- You can mirror the ingress or egress traffic that is associated with one or more subscriber hosts.
- You can specify match criteria, such as IP addresses, MAC addresses, or MPLS ingress labels, to filter the mirrored traffic.
- You can configure forwarding classes and profiles for mirror service traffic on supported devices.
- Mirror service IDs are obtained from the same pool of IDs that is used by other services. When you manually assign an ID value, ensure that you do not assign an ID that belongs to another service.
- Use the packet-slicing option to copy a specific packet size from each frame. This option is useful for monitoring network usage without copying the customer data. It also limits the amount of mirrored traffic that travels through the core network.

- When the mirror destination is not on the same NE as the mirror source, a mirror service requires a service tunnel between the source and destination NEs.
- The 5620 SAM can automatically create a service tunnel between the source and destination sites when the following conditions are met:
  - Automatic mesh SDP binding creation is enabled.
  - GRE or LDP is the transport type.
  - No other service tunnel is available between the source and destination sites.
- The mirror service source and destination encapsulation types must be the same.
- After an NE reboot or CPM activity switch, the debug configuration file for a mirror service is not by default reloaded on the NE. The 5620 SAM raises an alarm when this occurs. To ensure that the NE reloads the debug configuration file, you must specify the location of the file in the base 5620 SAM configuration. See "To enable debug configuration file reloading on an NE for mirror services" in the *5620 SAM System Administrator Guide* for more information.
- When multiple mirror services reference the same packet, for example, from a SAP and from a port, the packet is mirrored only once, based on the following criteria in the following non-configurable order:
  - MAC or IP filters
  - MPLS ingress label
  - SAP
  - port
- For IP-only mirroring, consider the following:
  - IP-only mirroring requires chassis mode C or D to be enabled.
  - By using "IP Only" as the encapsulation type, users can specify that only the IP packet is mirrored, without its original ATM/FR/POS/Ethernet DLC header.
  - When IP-only is configured on the source site, users can configure various mirroring sources, including subscribers and SAPs from Ipipe, IES, VPRN, VPLS, and MVPLS services. However, source ports and VLL services including Apipe, Epipe, and Fpipe cannot be configured.
  - For local IP-only mirroring, the source and destination MAC addresses must be configured.
  - For remote IP-only mirroring in a VPRN service, an IP mirror interface on the VPRN destination NE is used to receive the IP mirror packets and route them to the appropriate sniffer. If there are multiple sniffers connected to the VPRN using L3 interfaces, you must configure the routing policy to have IP mirror packets routed to the correct sniffer.
- For LI source configuration, consider the following:
  - You must be assigned the Lawful Interception Management scope of command role to view, create or modify any LI-related objects in the 5620 SAM.
  - LI source configurations are saved on an NE when the polling policy for the NE specifies LI Local Save Allowed. See chapter 9 for information about configuring in-band and out-of-band polling policies.

69.2 Sample mirror service configuration

Figure 69-1 shows a sample mirror service configuration.

Figure 69-1 Sample mirror service configuration



In this sample, Router B is the mirror source that carries the customer packets. Router A is the mirror destination. The ingress and egress traffic on Port 5/2/1 is mirrored on the destination, Port 3/1/3. Table 69-1 lists the high-level tasks to configure the sample mirror service.

Table 69-1 Sample mirror service configuration

Task	Description
1. Connect the packet sniffer to the mirror destination.	The packet sniffer is attached to Router A, Port 3/1/3.
2. Configure the mirror destination parameters.	Port 3/1/3 on Router A is specified as the mirror destination. Specify the Tunnel ID 1000 as the transport tunnel to the mirror destination. All the parameters required to configure the type of mirroring, for example, slicing and mirror classification, are specified in the destination parameters.
3. Specify the source entity that is to be mirrored.	The egress and ingress traffic on Port 5/2/1 is to be mirrored.

69.3 Workflow to create a mirror service

The following workflow lists the high-level steps required to create a mirror service. As a prerequisite for creating a mirror service, this workflow assumes the following:

- a group or customer with the required user access privileges has been configured.
- the IP or IP/MPLS core network exists.
- any required service tunnels are created including the static or dynamic LSP required to create the service tunnel; see Procedure 27-1.

- the access ports for the service are created; see chapter 16 for more information.
- any required pre-defined routing, QoS, scheduling, filter, accounting, and time of day suite policies are created; see chapter 42 for more information. You do not have to create pre-defined policies if policies are created on a per-service basis.
- any required MP-BGP for PE-to-PE routing is configured; see chapter 23 for more information about protocol configuration.
- the network services the mirror service will use are created.
- a packet-sniffing device at the L2 SAP that is the destination of the mirror service is configured.
- the SAP with the attached packet-sniffing device as the mirror destination is specified.
- the source of the packets to be mirrored is configured.

1 Create the mirror service. See Procedure 69-1.

i Define the general properties for the mirror service.

ii Specify the services for inclusion in the mirror service. You can specify multiple services in one operation.

iii Enable one or more routing protocols for the mirror site.

iv Create a destination site on the mirror service. See Procedure 69-2.

v Create a source site on the mirror service, if required. See Procedure 69-3.

vi Specify an endpoint on the site for redundancy, if required. See Procedure 69-5.

vii Create an L2 access interface on the destination site, if required. See Procedure 69-6.

viii Specify one or more SAPs on the site as a mirror source, if required. See Procedure 69-7.

ix Specify one or more ports on the site as a mirror source, if required. See Procedure 69-8.

x Specify one or more IP filters for the source site, if required. See Procedure 69-9.

xi Specify one or more IPv6 filters for the source site, if required. See Procedure 69-10.

xii Specify one or more MAC filters for the source site, if required. See Procedure 69-11.

xiii Specify one or more LI source MAC filters for the source site, if required. See Procedure 69-12.

xiv Specify one or more MPLS ingress labels for the source site, if required. See Procedure 69-13.

xv Specify one or more subscribers or subscriber hosts as mirror sources, if required. See Procedure 69-14.

xvi Turn up the mirror service.

2 As required, view mirror service information:

a View the service topology map associated with a Mirror Service. See Procedure 69-15.

b View the mirror service operational status. See Procedure 69-16.

c To view LI mirrored subscriber hosts configured with a RADIUS server. See Procedure 69-17.

3 As required, run an OAM validation test for a mirror service. See Procedure 69-19.

4 As required, modify a mirror service. See Procedure 69-20.

5 As required, delete a mirror service. See Procedure 69-21.

69.4 Mirror service procedures

Use the following procedures to create, delete, view, and modify mirror services.



Note 1 — If you are configuring mirror services using dot1q or qinq SAPs on a 7210 SAS (except for a 7210 SAS-D), you must first assign a mirror port. See Procedure 69-18.

Note 2 — On the 7210 SAS-X only, you can also configure access egress policies.

Procedure 69-1 To create a mirror service

1 Choose Create→Service→Mirror from the 5620 SAM main menu. The Mirror Service (Create) form opens with the General tab displayed.

2 Configure the parameters:

- Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Auto-Assign ID
- SVC Mgr Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Service Name
- Description
- Service Tier
- Service Priority
- Administrative State

3 Perform one of the following:

a Leave the Automatic SDP Binding Creation parameter disabled.

When you leave the Automatic SDP Binding Creation parameter disabled, you must create SDP bindings for the service and bind the SDPs to a service tunnel in step 18 of Procedure 69-3.

b Enable the Automatic SDP Binding Creation parameter.

When you enable the Automatic SDP Binding Creation parameter, SDP bindings for the service are automatically created and bound to service tunnels.

i Configure the Transport Type parameter.



Note 1 — You must select GRE or LDP as the transport type to allow the 5620 SAM to automatically create SDP bindings between the source and destination sites. Automatic creation of SDP bindings cannot be configured if a service tunnel already exists between the source and destination sites.

Note 2 — To use MPLS:RSVP as the transport type, you must bind LSPs to service tunnels during service tunnel configuration. See chapter 27 for more information.

ii Configure the Use Bandwidth-Reserved Paths parameter, if applicable.

The Use Bandwidth-Reserved Paths parameter is configurable only when the Transport Type parameter is set to MPLS:RSVP or Any.

4 Configure the OLC state:

i Click on the Apply button.

ii Configure the parameters:

- Current OLC State
- Revert OLC State

5 To configure a mirror source on a destination site, perform steps 4 to 25 of Procedure 69-2.

6 To configure a mirror source on a site other than the destination site, perform steps 4 to 18 of Procedure 69-3. Otherwise, go to step 7.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The Mirror Service (Create) form closes.

Procedure 69-2 To create a destination site on a mirror service

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria and click the Search button. A list of mirror services appears.

3 Select a mirror service and click on the Properties button. The Mirror Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, right-click on Destination Site and choose Create Destination Site from the contextual menu. The Select Network Elements - Mirror Service form opens with a list of available sites displayed.

5 Select a site and click on the OK button. The Select Network Elements - Mirror Service form closes and the Mirror Site (Create) form opens with the system identifier of the selected site displayed in the Network Element panel.

6 Configure the parameters.

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State

7 Configure the NE-specific parameters, as listed in Table 69-2.

Table 69-2 NE-specific parameters

NE	Parameters	Dependencies
7450 ESS, 7710 SR, 7750 SR, and 7950 XRS	• Encapsulation Type	No dependencies.

8 Click on the Mirroring Configuration tab.

9 Configure the parameters:

- Source Administrative State
- Remote Source Capable

10 Configure the NE-specific parameters, as listed in Table 69-3.

Table 69-3 NE-specific parameters

NE	Parameters	Dependencies
7450 ESS, 7710 SR, 7750 SR, 7950 XRS	• Slice Size • Enable Port ID Mirroring	Choose the default of 0 for the Slice Size parameter when you configure a destination mirror site, unless slicing at the destination is necessary. Packet slicing reduces the amount of mirrored traffic that traverses the network. The Slice Size parameter is not displayed if the Encapsulation Type parameter is set to IP Only. The Port Id Mirroring and remote source are mutually exclusive. If Enable Port ID Mirroring is set to true on the destination site, then a remote source site cannot be added to the service. If a remote source site is already on the service, then Enable Port ID Mirroring cannot be set to true. Also, if remote mirror is used, then Enable Port ID Mirroring must be configured on all source sites. The Enable Port ID Mirroring parameter is configurable only if the Encapsulation Type parameter is set to PPP.
7210 SAS-D, 7210 SAS-E, 7210 SAS-M, 7210 SAS-T, 7210 SAS-X, 7450 ESS, 7710 SR, 7750 SR, 7950 XRS	• Forwarding Class	If you are configuring a 7210 SAS-X, go to step 16. If you are configuring a 7450 ESS, 7710 SR, 7750 SR, or 7950 XRS, Release 10.0 or earlier, go to step 11.
7210 SAS-D, 7210 SAS-E, 7210 SAS-M, 7210 SAS-T	• Profile	Go to step 16.

11 Click on the Source Far Ends tab.

12 Click on the Create button. The Remote Source (Create) form appears.

13 Configure the parameters:

- Remote Site ID
- Ingress Label
- Remote VC ID
- Remote ICB

14 Click on the OK button. The Remote Source (Create) form closes and a dialog box appears.

15 Click on the OK button. The Mirror Site (Create) form displays the remote source information.

16 Click on the OK button on the Mirror Site (Create) form. A dialog box appears.

17 Click on the OK button. The Mirror Service (Edit) form reappears with the service navigation tree displayed.

18 To add an L2 access interface, see Procedure 69-6.

19 To specify an endpoint on the site for redundancy, perform steps 5 to 18 of Procedure 69-5.

20 A mirror source can be on the same site as the mirror destination. If no mirror sources are on the destination site, go to Procedure 69-3.

21 To specify one or more SAPs on the site as mirror sources, perform steps 5 to 11 of Procedure 69-7.

22 To specify one or more ports on the site as mirror sources, perform steps 5 to 11 of Procedure 69-8.

23 To specify one or more IP filters for the source site, perform steps 4 to 11 of Procedure 69-9.

24 To specify one or more MAC filters for the source site, perform steps 4 to 11 of Procedure 69-11.

25 To specify one or more LI source LI MAC filter for the source site, perform steps 4 to 11 of Procedure 69-12.

Procedure 69-3 To create a source site on a mirror service

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria and click the Search button. A list of mirror services appears.

3 Select a mirror service and click on the Properties button. The Mirror Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, right-click on Source Site and choose Create Source Site from the contextual menu. The Select Network Elements - Mirror Service form opens with a list of available sites displayed.

5 Select a site and click on the OK button. The Select Network Elements - Mirror form closes and the Mirror Site (Create) form opens with the system identifier of the selected site displayed.

6 Configure the parameters.

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State
- Encapsulation Type

7 Click on the Mirroring Configuration tab.

8 Configure the parameters.

- Source Administrative State
- Remote Source Capable
- Slice Size
- Forwarding Class
- Enable Port ID Mirroring



Note 1 — The Slice Size parameter is not displayed if the Encapsulation Type parameter is set to IP Only.

Note 2 — The Enable Port ID Mirroring parameter is configurable only if you set the Encapsulation Type parameter to PPP in step 6.

The Port Id Mirroring and remote source are mutually exclusive. If Enable Port ID Mirroring is set to true on the destination site, then a remote source site cannot be added to the service. On the other hand, if a remote source site is already on the service, then Enable Port ID Mirroring cannot be set to true. Also, if remote mirror is used, then Enable Port ID Mirroring must be configured on all source sites.

9 Click on the L3 Encapsulation tab, if required. Otherwise, go to step 15.



Note — The L3 Encapsulation tab appears only if you are configuring a source site on an NE in chassis mode D. See chapter 15 for more information about chassis modes.

You can configure an Layer 3 encapsulation option to allow LI-mirrored packets to be placed into a routable header (either IP-UDP Shim or IP-GRE) and then forwarded in a routing context.



Note — The following conditions apply if you configure the Layer 3 encapsulation option:

- Configuring Mirror SDP bindings and Mirror SAPs is mutually exclusive to the L3 Encapsulation
- You cannot configure the Session ID or Intercept ID of a source later on in this procedure if the L3 Encapsulation is not configured here.
- You cannot configure L3 Encapsulation if a mirror source object (such as: IP filter, MAC filter, and so on) is first configured for this service.
- You cannot change the routing instance of L3 Encapsulation if a gateway is first configured for this service.

10 Click on the Create button. The Layer-3 Encapsulation null (Create) form appears.

11 Configure the parameters:

- Header Type
- Use Direction Bit

  The Use Direction Bit parameter is only displayed if you configured the Header Type option for IP-UDP Shim.

12 Click on the Select button to choose a Routing Instance ID.

The Select Routing Instance - Layer-3 Encapsulation - null form opens.

13 Choose the required instance from the list and click the OK button.

The Select Routing Instance - Layer-3 Encapsulation - null form closes and the Layer-3 Encapsulation null (Create) form displays your selection.

14 Configure a Gateway by performing the following in the Gateway panel:

i Click the Create button in the Gateway panel. The Layer-3 Encapsulation Gateway null (Create) form is displayed.

ii Configure the parameters.

- Source Address
- Destination Address
- Source Port
- Destination Port

The gateway Source Address and Destination Address must either both be unconfigured or both configured. Similarly, the gateway Source Port and Destination Port must either both be unconfigured or both configured.

The Source Port and Destination Port parameters are displayed only if you configured the Header Type option for IP-UDP Shim.

iii Click on the OK button. The Layer-3 Encapsulation Gateway null (Create) form closes and a confirmation message is displayed.

iv Click on the OK button. The new gateway appears in the list.

v Click on the OK button. The Layer-3 Encapsulation null (Create) form closes and a confirmation message is displayed.

vi Click on the OK button. The L3 encapsulation option appears in the list.

15 Click on the OK button. A dialog box appears.

16 Click on the OK button. The Mirror Site (Create) form closes, and the Mirror Service (Create) form reappears with the selected site displayed on the navigation tree under Source Sites.

17 Expand the newly created site object.

18 Perform one of the following:

a If the Automatic SDP Binding Creation parameter was disabled in step 3, choose an SDP binding for the mirror source by selecting Mirror SDP Binding under the source site in the service navigation tree and then right-clicking and choosing Create Mirror SDP Binding from the contextual menu.

b Go to step 25.

19 The Mirror SDP Binding (Create) form opens. Specify a destination NE for the mesh SDP binding:

a If the destination NE is a managed NE, choose from a list of managed NEs.

i Click on the Select button beside the Tunnel Termination Site parameter to choose a destination for the SDP binding. The Select Destination Network Element - Mirror SDP Binding form opens.

ii Select a NE and click on the OK button. The Select Destination Network Element - Mirror SDP Binding form closes and the Mirror SDP Binding (Create) form displays the destination NE ID in the Tunnel Termination Site panel.

b If the destination NE is not managed by the 5620 SAM, specify the system ID of the destination NE for the Tunnel Termination Site parameter.

20 Configure the parameters.

- VC ID
- Auto-Assign ID
- Ingress Label
- Egress Label
- Inter-Chassis Backup
- Precedence

21 Perform one of the following to specify a transport tunnel for the mirror SDP binding.

a Let the 5620 SAM configure the transport tunnel automatically.

i Enable the Auto-Select Transport Tunnel parameter.

ii Configure the Tunnel Auto-Selection Transport Preference parameter.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Mirror SDP Binding form opens.

ii Select a service tunnel for the mirror SDP binding and click on the OK button. The Select Tunnel - Mirror SDP Binding form closes, and the Mirror SDP Binding (Create) form displays the service tunnel identifier.

c Configure an MPLS-TP transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Mirror SDP Binding form opens.

ii Select an MPLS-TP service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Mirror SDP Binding form closes, and the Mirror SDP Binding (Create) form refreshes with the service tunnel identifier. See Procedure 27-1 for more information about how to create an MPLS-TP service tunnel.

22 Click on the Pseudowire OAM tab and configure the Control Word parameter.



Note — If you are creating a mirror SDP binding using an MPLS-TP service tunnel for pseudowire static configuration, you must set the Control Word parameter to Preferred. See Procedure 69-4.

23 Click on the OK button. A dialog box appears.

24 Click on the OK button. The Mirror SDP Binding (Create) form closes and the Mirror Service (Create) form displays the mirror SDP binding under Mirror SDP Binding for the site.

25 To specify an endpoint on the site for redundancy, perform steps 5 to 18 of Procedure 69-5.

26 To specify one or more SAPs on the site as mirror sources, perform steps 5 to 11 of Procedure 69-7.

27 To specify one or more ports on the site as mirror sources, perform steps 5 to 11 of Procedure 69-8.

28 To specify one or more IP filters for the source site, perform steps 4 to 11 of Procedure 69-9.

29 To specify one or more MAC filters for the source site, perform steps 4 to 11 of Procedure 69-11.

30 To specify one or more LI source LI MAC filter for the source site, perform steps 4 to 11 of Procedure 69-12.

31 To specify one or more MPLS ingress labels for the source site, perform steps 4 to 9 of Procedure 69-13.

32 To specify one or more subscribers or subscriber hosts as a mirror source, perform steps 4 to 11 of Procedure 69-14.

Procedure 69-4 To configure an MPLS-TP static pseudowire on a mirror SDP binding

Perform this procedure to create an MPLS-TP static pseudowire on the mirror SDP binding. An MPLS-TP service tunnel must be used in the mirror SDP binding, and the Control Word parameter for pseudowire OAM must be set to Preferred in step 22 of Procedure 69-3.

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria and click on the Search button. A list of mirror services appears.

3 Select a miror service and click on the Properties button. The Mirror Service (Edit) form opens.

4 On the navigation tree, expand the source site on which you want to configure the mirror SDP binding, and expand the Mirror SDP Bindings icon.

5 Click on the mirror SDP binding on which you want to configure the static MPLS-TP pseudowire. The Mirror SDP Binding (Edit) form opens with the General tab displayed.

6 Click on the Control Channel tab.

7 Configure the parameters:

- Status
- Refresh Timer (seconds)
- Request Timer (seconds)

8 Click on the MPLS-TP PW tab.

9 Click on the Create button. The PW Path ID (Create) form opens.

10 Configure the Path AGI parameter.

11 Configure the parameters in the Source Attachment Individual Identifier panel:

- SAII Global ID
- SAII Node ID
- SAII AC ID

12 Configure the parameters in the Target Attachment Individual Identifier panel:

- TAII Global ID
- TAII Node ID
- TAII AC ID

13 Click on the OK button. The PW Path ID (Create) form closes.

14 Click on the OK button. The Mirror SDP Binding (Edit) form closes.

15 Close the Mirror Service (Edit) form.

16 Close the Manage Mirror Services form.

Procedure 69-5 To create an endpoint for redundancy support on the site

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria and click the Search button. A list of mirror services appears.

3 Select a mirror service and click on the Properties button. The Mirror Service (Edit) form opens with the General tab displayed.

4 Perform one of the following.

a To create an endpoint on a destination site, expand the Destination Site object to view the configured destination sites, and expand the destination site object on which you are creating the endpoint.

b To create an endpoint on a source site, expand the Source Site object to view the configured source sites, and expand the source site object on which you are creating the endpoint.

5 On the navigation tree, right-click on the Endpoints object below the site and choose Create Endpoints. The Endpoint (Create) form opens.

6 Configure the parameters.

- Name
- Description
- Revert Time (seconds)
- Disable Revert Time

7 Click on the OK button.

For the destination site, the L2 Access Interface (Test Equipment Interface) and Mirror SDP Binding objects appear under the Endpoints object.

For the source site, the Mirror SDP Binding object now appears under the Endpoints object.

8 To create an L2 access interface as the mirror destination, right-click on the L2 Access Interface (Test Equipment Interface) object under the Endpoints object and choose Create L2 Access Interface from the contextual menu. The L2 Access Interface (Create) form opens with the General tab displayed.



Note — You cannot create an L2 access interface on the endpoint if you create an L2 access interface in Procedure 69-6 without selecting an endpoint for redundancy.

9 Click on the Port tab.

10 Click on the Select button to choose a port for the L2 access interface. The Select Terminating Port - L2 Access Interface form opens.

11 Use the configurable filter and Search button to choose a port, and click on the Search button. The Select Terminating Port - L2 Access Interface form closes, and the L2 Access Interface (Create) form displays the port information.



Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

12 Configure other parameters, as required.

13 Click on the OK button on the L2 Access Interface (Create) form. The form closes and a dialog box appears.

14 Click on the OK button. The SAP object appears under the L2 Access Interface object.

15 To create a mirror SDP binding on the endpoint, right-click on the Mirror SDP Binding object under the Endpoints object in the service navigation tree and choose Create Mirror SDP Binding from the contextual menu. The Mirror SDP Binding (Create) form opens.

16 Configure the parameters.

- Tunnel Termination Site
- VC ID
- Auto-Assign ID
- Ingress Label
- Egress Label
- Inter-Chassis Backup
- Precedence

17 Click on the OK button. The Mirror SDP Binding (Create) form closes and a dialog box appears.

18 Click on the OK button. The Mirror Service (Edit) form reappears with the service navigation tree displayed.

Procedure 69-6 To create an L2 access interface on a destination site



Note — You cannot create an L2 access interface on the site if you create an L2 access interface for redundancy in Procedure 69-5.

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria and click the Search button. A list of mirror services appears.

3 Select a mirror service and click on the Properties button. The Mirror Service (Edit) form opens with the General tab displayed.

4 Expand the Destination Site object to view the destination sites.

5 Expand the destination site object on which you are creating the L2 access interface.

6 Configure an L2 access interface as the mirror destination by right-clicking on L2 Access Interface (Test Equipment Interface) under the destination site in the service navigation tree and choosing Create L2 Access Interface from the contextual menu. The L2 Access Interface (Create) form opens with the General tab displayed.

7 To configure an endpoint for redundancy, click on the Select button in the Redundancy panel to select the desired endpoint from the drop-down menu. Otherwise, go to step 8.



Note — If you select an endpoint for redundancy, the L2 access interface appears under the Endpoints object on the service navigation tree.

8 Click on the Port tab.

9 Click on the Select button in the Terminating Port panel to choose a port for the L2 access interface. The Select Terminating Port - L2 Access Interface form opens.

10 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - L2 Access Interface form closes, and the L2 Access Interface (Create) form displays the port information.



Note 1 — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

Note 2 — The form lists only ports that have the encapsulation type that you specified in the destination site creation, in Procedure 69-2

11 Configure the parameters.

- Outer Encapsulation Value
- Auto-Assign ID
- Inner Encapsulation Value

The Auto-Assign ID parameter is configurable if the port uses dot1q encapsulation. When the parameter is enabled, the 5620 SAM automatically configures the Outer Encapsulation Value parameter using the lowest unassigned value.



Note — You can set the Auto-Assign ID parameter to be the default parameter for dot1q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter on the User Preferences form.

The Inner Encapsulation Value is configurable only when the port is an Ethernet or frame relay port with QinQ encapsulation.

12 Assign an egress QoS policy to the interface, if required.

i Click on the QoS tab.

ii Configure the Egress Mark QinQ Top Bits Only parameter.

iii Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - L2 Access Interface form opens.

iv Configure the filter criteria. A list of egress policies appear at the bottom of the Select Egress Policy - L2 Access Interface form.

v Select an egress policy and click on the OK button. The Select Egress Policy - L2 Access Interface form closes and the L2 Access Interface (Create) form displays the egress QoS policy information.

13 Assign a time of day suite to the interface, if required.

i Click on the TOD Suite tab.

ii Click on the Select button beside the Name parameter. The Select Time Of Day Suite - L2 Access Interface form opens.

iii Select a time of day suite and click on the OK button. The Select Time Of Day Suite - L2 Access Interface form closes and the L2 Access Interface (Create) form displays the time of day suite information.

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Mirror (Create) form displays the L2 access interface information below L2 Access Interface (Test Equipment Interface) in the service navigation tree.

14 Click on the Schedulers tab, if required.

15 Configure the Aggregate Rate Limit (kbps) parameter.

16 Click on the IP Mirror MAC Addresses tab, if you are configuring local mirroring and you chose IP Only as the encapsulation type in step 6 of Procedure 69-2. Otherwise, go to step 18.



Note — If you want to configure remote mirroring in a VPRN service, you must create an IP Mirror Interface in that service. See chapter 71 for more information.

17 Configure the parameters:

- Destination MAC Address
- Source MAC Address



Note — The Source and Destination MAC addresses on L2 Access Interface must be both null or neither null. Both null means that there are no source or destination MAC addresses configured on the interface.

18 Assign an ANCP policy to the interface, if required.

i Click on the ANCP Static Map tab.

ii Click on the Create button. The ANCP Static Map (Create) form opens.

iii Configure the ANCP String parameter.

iv Click on the Select button to choose an ANCP Policy. The Select ANCP Policy - ANCP Static Map form opens.

v Select an ANCP policy and click on the OK button. The Select ANCP Policy - ANCP Static Map form closes and the ANCP Static Map form reappears with the ANCP policy information displayed.

vi Click on the OK button. The ANCP Static Map form closes.

19 Click on the OK button. A dialog box appears.

20 Click on the OK button. The L2 Access Interface (Create) form closes.

Procedure 69-7 To specify a SAP on the site as a mirror source

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria and click the Search button. A list of mirror services appears.

3 Select a mirror service and click on the Properties button. The Mirror Service (Edit) form opens with the General tab displayed.

4 Perform one of the following.

a To create a source interface on a destination site, expand the Destination Site object to view the configured destination sites, and expand the destination site object on which you are creating the source SAP.

b To create a source interface on a source site, expand the Source Site object to view the configured source sites, and expand the source site object on which you are creating the source SAP.

5 Perform one of the following:

a Right-click on the Source SAPs object below the site in the service navigation tree and choose Create Source Interface from the contextual menu. The Source Interface (Create) form opens. Go to step 6.

b Right-click on the LI Source SAPs object below the site in the service navigation tree and choose Create LI Source Interface from the contextual menu. The LI Source Interface (Create) form opens. Go to step 6.



Note 1 — A 5620 SAM operator with LI privileges can view, create, and delete LI source objects.

Note 2 — A mirror site can be configured with debug or LI sources, but not both. LI source configuration takes priority over debug source configuration.

6 Click on the Select button to choose an access interface to associate with the source interface. The Select Mirrored Interface - Source Interface form opens.

7 Use the configurable filter and Search button to choose an access interface, and click on the OK button. The Select Mirrored Interface - Source Interface form closes and the Source Interface (Create) form displays the selected interface information.

8 Configure the parameters:

- Enable Egress
- Enable Ingress
- Intercept ID
- Session ID

The Intercept ID and Session ID parameters are displayed only when creating an LI source SAP.

9 Click on the OK button. A dialog box appears.

10 Click on the OK button. The Mirror Service (Edit) form displays the source SAP below Source SAPs in the service navigation tree.

11 Repeat steps 6 to 10 to specify an additional source SAP for the site.

Procedure 69-8 To specify a port on the site as a mirror source

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria and click the Search button. A list of mirror services appears.

3 Select a mirror service and click on the Properties button. The Mirror Service (Edit) form opens with the General tab displayed.

4 Perform one of the following.

a To create a source port on a destination site, expand the Destination Site object to view the configured destination sites, and expand the destination site object on which you are creating the source port.

b To create a source port on a source site, expand the Source Site object to view the configured source sites, and expand the source site object on which you are creating the source port.

5 Right-click on the Source Ports object below the site in the service navigation tree and choose Create Source Port from the contextual menu. the Source Port (Create) form opens

6 Click on the Select button to choose a port. The Select - Source Port form opens.

A source port can be one of the following:

- physical port
- channel
- LAG
- bundle
- CCAG

7 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Source Port form closes and the Source Port (Create) form displays the port information.

8 Configure the parameters:

- Enable Egress
- Enable Ingress

9 Click on the OK button. A dialog box appears.

10 Click on the OK button. The Mirror Service (Create) form displays the source port below Source Ports in the service navigation tree.

11 Repeat steps 5 to 10 to specify an additional source port for the site.

Procedure 69-9 To specify a source IP or LI source IP filter entry for the mirror source

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria and click the Search button. A list of mirror services appears.

3 Select a mirror service and click on the Properties button. The Mirror Service (Edit) form opens with the General tab displayed.

4 Perform one of the following.

a To specify an IP filter entry on a destination site, expand the Destination Site object to view the configured destination sites, and expand the destination site object on which you are specifying the IP filter entry.

b To specify an IP filter entry on a source site, expand the Source Site object to view the configured source sites, and expand the source site object on which you are specifying the IP filter entry.

5 Perform one of the following:

a Right-click on the Source IP Filters object below the site in the service navigation tree and choose Create Source IP Filter from the contextual menu. The Source IP Filter (Create) form opens. Go to step 6.

b Right-click on the LI Source IP Filters object below the site in the service navigation tree and choose Create LI Source IP Filter from the contextual menu. The LI Source IP Filter (Create) form opens. Go to step 6.



Note 1 — A 5620 SAM operator with LI privileges can view, create, and delete LI source objects.

Note 2 — A mirror site can be configured with debug or LI sources, but not both. LI source configuration takes priority over debug source configuration.

6 Click on the Select button to choose an IP filter entry. The Select Filter - Source IP Filter form opens.

7 Use the configurable filter and Search button to choose an IP filter entry, and click on the OK button. The Select Filter - Source IP Filter form closes and the Source IP Filter (Create) form displays the selected IP filter ID and IP filter entry ID.

8 If you are configuring an LI source IP filter, configure the parameters. Otherwise, go to step 9.

- Intercept ID
- Session ID

The Intercept ID and Session ID parameters are displayed only when creating an LI source IP filter.

9 Click on the OK button. A dialog box appears.

10 Click on the OK button. The Mirror (Create) form displays the source IP filter below Source IP Filters in the service navigation tree.

11 Repeat steps 6 to 10 to specify an additional source IP filter.

Procedure 69-10 To specify a source IPv6 or LI source IPv6 filter entry for the mirror source

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria and click the Search button. A list of mirror services appears.

3 Select a mirror service and click on the Properties button. The Mirror Service (Edit) form opens with the General tab displayed.

4 Perform one of the following.

a To specify an IPv6 filter entry on a destination site, expand the Destination Site object to view the configured destination sites, and expand the destination site object on which you are specifying the IPv6 filter entry.

b To specify an IPv6 filter entry on a source site, expand the Source Site object to view the configured source sites, and expand the source site object on which you are specifying the IPv6 filter entry.

5 Perform one of the following:

a Right-click on the Source IPv6 Filters object below the site in the service navigation tree and choose Create Source IPv6 Filter from the contextual menu. The Source IPv6 Filter (Create) form opens.

b Right-click on the LI Source IPv6 Filters object below the site in the service navigation tree and choose Create LI Source IPv6 Filter from the contextual menu. The LI Source IPv6 Filter (Create) form opens.



Note 1 — A 5620 SAM operator with LI privileges can view, create, and delete LI source objects.

Note 2 — A mirror site can be configured with debug or LI sources, but not both. LI source configuration takes priority over debug source configuration.

6 Click on the Select button to choose an IPv6 filter entry. The Select Filter - Source IPv6 Filter form opens.

7 Use the configurable filter and Search button to choose an IPv6 filter entry, and click on the OK button. The Select Filter - Source IPv6 Filter form closes and the Source IPv6 Filter (Create) form displays the selected IPv6 filter ID and IPv6 filter entry ID.

8 If you are configuring an LI source IPv6 filter, configure the parameters. Otherwise, go to step 9.

- Intercept ID
- Session ID

The Intercept ID and Session ID parameters are configurable only if Layer 3 encapsulation is configured on the mirror site. See Procedure 69-2.

9 Click on the OK button. A dialog box appears.

10 Click on the OK button. The Mirror (Create) form displays the source IPv6 filter below Source IPv6 Filters or LI Source IPv6 Filters in the service navigation tree.

11 Repeat steps 6 to 10 to specify an additional source or LI source IPv6 filter.

Procedure 69-11 To specify a source MAC or LI source MAC filter entry for the mirror site

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria and click the Search button. A list of mirror services appears.

3 Select a mirror service and click on the Properties button. The Mirror Service (Edit) form opens with the General tab displayed.

4 Perform one of the following.

   a To specify a MAC filter entry on a destination site, expand the Destination Site object to view the configured destination sites, and expand the destination site object on which you are specifying the MAC filter entry.

   b To specify a MAC filter entry on a source site, expand the Source Site object to view the configured source sites, and expand the source site object on which you are specifying the MAC filter entry.

5 Perform one of the following:

   a Right-click on the Source MAC Filters object below the site in the service navigation tree and choose Create Source MAC Filter from the contextual menu. The Source MAC Filter (Create) form opens. Go to step 6.

   b Right-click on the LI Source MAC Filters object below the site in the service navigation tree and choose Create LI Source MAC Filter from the contextual menu. The LI Source MAC Filter (Create) form opens. Go to step 6.



Note 1 — A 5620 SAM operator with LI privileges can view, create, and delete LI source objects.

Note 2 — A mirror site can be configured with debug or LI sources, but not both. LI source configuration takes priority over debug source configuration.

6 Click on the Select button to choose a MAC filter entry. The Select Filter - Source Mac Filter form opens.

7 Use the configurable filter and Search button to choose a MAC filter entry, and click on the OK button. The Select Filter - Source Mac Filter form closes and the Source MAC Filter (Create) form displays the selected MAC filter ID and MAC filter entry ID.

8 Configure the parameters:

- Intercept ID
- Session ID

The Intercept ID and Session ID parameters are displayed only when creating an LI source MAC filter.

9 Click on the OK button. A dialog box appears.

10 Click on the OK button. The Mirror (Create) form displays the source MAC filter below Source MAC Filters in the service navigation tree.

11 Repeat steps 6 to 10 to specify an additional source MAC filter.

Procedure 69-12 To specify an LI source LI MAC filter for the mirror site

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria and click the Search button. A list of mirror services appears.

3 Select a mirror service and click on the Properties button. The Mirror Service (Edit) form opens with the General tab displayed.

4 Perform one of the following.

a To specify an LI MAC filter entry on a destination site, expand the Destination Site object to view the configured destination sites, and expand the destination site object on which you are specifying the LI MAC filter entry.

b To specify an LI MAC filter entry on a source site, expand the Source Site object to view the configured source sites, and expand the source site object on which you are specifying the LI MAC filter entry.

5 Right-click on the LI Source LI MAC Filters object below the site in the service navigation tree and choose Create LI Source LI MAC Filter from the contextual menu. The LI Source LI MAC Filter (Create) form opens.



Note 1 — A 5620 SAM operator with LI privileges can view, create, and delete LI source objects.

Note 2 — A mirror site can be configured with debug or LI sources, but not both. LI source configuration takes priority over debug source configuration.

6 Click on the Select button to choose an LI MAC filter entry. The Select LI MAC Filter Entry - LI Source LI MAC Filter form opens.

7 Use the configurable filter and Search button to choose an LI MAC filter entry, and click on the OK button. The Select LI MAC Filter Entry - LI Source LI MAC Filter form closes and the LI Source LI MAC Filter (Create) form displays the selected Filter Name and Filter Entry ID.

8 Configure the parameters:

- Intercept ID
- Session ID

The Intercept ID and Session ID parameters are displayed only when creating an LI source MAC filter.

9 Click on the OK button. A dialog box appears.

10 Click on the OK button. The Mirror (Create) form displays the LI Source LI MAC filter below LI Source LI MAC Filters in the service navigation tree.

11 Repeat steps 5 to 10 to specify an additional LI source LI MAC filter.

Procedure 69-13 To specify an MPLS ingress label for the mirror

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria and click the Search button. A list of mirror services appears.

3 Select a mirror service and click on the Properties button. The Mirror Service (Edit) form opens with the General tab displayed.

4 Expand the Source Site object to view the configured source sites, and expand the source site object on which you are specifying the MPLS ingress label.

5 Right-click on the Source MPLS Ingress Labels object below the site in the service navigation tree and choose Create Source Ingress Label from the contextual menu. The Source Ingress Label (Create) form opens.

6 Configure the Ingress Label parameter.

7 Click on the OK button. A dialog box appears.

8 Click on the OK button. The Mirror (Create) form displays the MPLS ingress label below Source MPLS Ingress Labels in the service navigation tree.

9 Repeat steps 5 to 8 to specify an additional source MPLS ingress label.

Procedure 69-14 To specify a source subscriber or LI source subscriber as a mirror source

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria and click the Search button. A list of mirror services appears.

3 Select a mirror service and click on the Properties button. The Mirror Service (Edit) form opens with the General tab displayed.

4 Expand the Source Site object to view the configured source sites, and expand the source site object on which you are specifying the subscriber as the mirror source.

5 Perform one of the following:

a Right-click on the Source Subscribers object below the site in the service navigation tree and choose Create Source Subscriber from the contextual menu. The Source Subscriber (Create) form opens. Go to step 6.

b Right-click on the LI Source Subscribers object below the site in the service navigation tree and choose Create LI Source Subscriber from the contextual menu. The LI Source Subscriber (Create) form opens. Go to step 6.



Note 1 — A 5620 SAM operator with LI privileges can view, create, and delete LI source objects.

Note 2 — A mirror site can be configured with debug or LI sources, but not both. LI source configuration takes priority over debug source configuration.

6 Configure the following parameters:

- Subscriber Identification String
- Forwarding Classes
- Enable Egress
- Enable Ingress
- Intercept ID
- Session ID

The Intercept ID and Session ID parameters are displayed only when creating an LI source subscriber.

7 You can further restrict the mirrored subscriber host traffic associated with the subscriber identification string by specifying SAP or SLA-profile criteria. To specify an SLA profile as a match criterion, go to step 13.



Note — You can configure parameters in the SAP/Subscriber Host Match Criteria panel or the SLA Profile Match Criteria panel, but you cannot configure parameters in both panels.

8 Click on the Select button in the SAP/Subscriber Host Match Criteria panel to specify a SAP on which to mirror subscriber host traffic. The Select SAP ID/Encap Value - Source Subscriber form opens.

9 Configure the filter criteria and click on the Select button. A list of SAPs is displayed.



Note — The form lists only dot1q- or QinQ-encapsulated SAPs that have subscriber management enabled.

10 Select a SAP in the list and click on the OK button. The Select SAP ID/Encap Value - Source Subscriber form closes and the SAP information is displayed on the Source Subscriber (Create) form.

11 Configure the parameters in the SAP/Subscriber Host Match Criteria panel to specify the subscriber host match criteria for the SAP:

- Host IP Address
- Host MAC Address



Note — The 5620 SAM does not accept the parameter values unless a SAP is specified in step 10.

12 Go to step 15.

13 Click on the Select button in the SLA Profile Match Criteria panel. The SLA Profile - Source Subscriber form opens.

14 Select an SLA profile in the list and click on the OK button. The Select SLA Profile - Source Subscriber form closes and the SLA profile name is displayed on the Source Subscriber (Create) form.

15 Click on the OK button. A dialog box appears.

16 Click on the OK button. The Mirror Service (Create) form displays the source subscriber below Source Subscribers in the service navigation tree.

17 Repeat steps 13 to 16 to specify an additional source subscriber, if required.

Procedure 69-15 To view the service topology associated with a mirror service

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter parameters and click on the Search button. A list of mirror services appears at the bottom of the Manage Mirror Services form.

3 Select a mirror service and click on the Topology View button. A Topology View dialog box appears.

4 Click on the Yes button to proceed. The Service Topology - *Service Name* map opens.

See chapter 6 for more information about service topology views.

Procedure 69-16 To view the mirror service operational status

The Aggregated Service Site Operational State and State Cause indicators on the General tab of the mirror service properties form display information about service faults.

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria. A list of mirror services appears at the bottom of the Manage Mirror Services form.

3 Select a mirror service and click on the Properties button. The Mirror *Service Name* (Edit) form opens.

4 View the Aggregated Service Site Operational State and State Cause indicators. When the Aggregated Operational State is Down or Partially Down, a check mark beside the appropriate State Cause indicator identifies the type of associated service fault.

5 Click on the appropriate tab to view or edit an object that is identified as faulty by a State Cause indicator.

6 Click on the Faults tab to view the alarms for the object. The alarms are grouped into various categories.

7 Close the Mirror Service (Edit) form.

8 Close the Manage Mirror Services form.

Procedure 69-17 To view LI mirrored subscriber hosts configured with a RADIUS server



Note 1 — You must have 5620 SAM LI user privileges to perform this procedure.

Note 2 — Before you can perform this procedure, at least one LI user account must exist on the NE.

Note 3 — Before you can perform this procedure, a 5620 SAM LI user must enable LI discovery for the NE using Procedure 28-8.

Note 4 — Only PPPoE subscriber hosts can be mirrored with RADIUS.

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria, if required, and click on the Search button. A list of mirror services appears.

3 Choose a mirror service and click on the Properties button. The Mirror *Service Name* (Edit) form opens with the General tab displayed.

4 Click on the Sites tab. A list of mirror service sites is displayed.

5 Choose a site and click on the Properties button. The Mirror Site (Edit) form opens with the General tab displayed.

6 If an LI source configuration object has not been created, the LI Source Configuration tab is dimmed. Click on the Create LI Source Configuration button at the bottom of the form. A dialog box appears.



Note 1 — You must create an LI source configuration object for the NE to mirror subscriber hosts for LI.

Note 2 — The Create LI Source Configuration button is a toggle that also lets you delete an LI source configuration object. If you delete an LI source configuration object, all associated LI source objects are deleted.

Note 3 — An LI source configuration object is automatically created when an LI source object is created.

7 Click on the OK button. The LI Source Configuration tab is enabled, and an LI source configuration object is created.

8 Click on the LI Source Subscribers Via RADIUS tab.

9 Configure the filter criteria, if required, and click on the Search button. A dialog box appears.

10 Click on the OK button. A list of subscribers appears.

11 Choose a subscriber and click on the Properties button. The LI Source Subscriber Host form opens.

12 View the information on the form.

13 Close the LI Source Subscriber Host form.

Procedure 69-18 To create a mirror port on a 7210 SAS

If you are creating a mirror service using qinq or dot1q SAPs, (except for the 7210 SAS-D) you must first create a mirror port.

1 Right-click on an NE in the Equipment view and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

2 Click on the Globals tab button.

3 Click on the Service tab button. The General sub-tab is displayed.

4 Click on the Select button in the Mirror Port panel. The Mirror Port form opens. Select a mirror port and click on the OK button. The Mirror Port form closes and the Mirror Port panel refreshes with the mirror port ID.

Procedure 69-19 To run an OAM validation test for a mirror service

An OAM validator test suite must be created for the tested entity. See chapter 77 for more information about how to create an OAM validator test suite.

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Mirror Services form.

3 Select a service and click on the Properties button. The Mirror Service (Edit) form opens with the General tab displayed.

4 Click on the Validate button. If an OAM validator test suite is not associated to the service, a dialog box appears. Perform the following steps:

   i Click on the OK button to associate the service with an existing OAM validator test suite. The Choose Validator Test Suite form appears.

   ii Configure the filter criteria. A list of OAM validator test suites appears.

   iii Select an OAM validator test suite and click on the OK button. The Choose Validator Test Suite form closes.

5 View the State Cause indicators. When the validation test fails, a check mark appears beside the OAM Validation Failure indicator.

6 Click on the Tests tab.

7 Click on the Tested Entity Result tab.

8 Select an entry and click on the Properties button. The Tested Entity Result form opens and displays information about the validation test.

9 Close the Tested Entity Result form.

10 Close the Mirror Service (Edit) form.

11 Close the Manage Mirror Services form.

Procedure 69-20 To modify a mirror service



Caution — Modifying parameters can be service-affecting.

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria. A list of mirror services appears at the bottom of the Manage Mirror Services form.

3 Select a mirror service and click on the Properties button. The Mirror *Service Name* (Edit) form opens with the general properties of the service displayed on the General tab.

4 Click on the other tabs to edit additional properties, as required.

5 Modify the parameters on the appropriate tab, as required.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button to confirm the action. The Mirror *Service Name* (Edit) form closes and the Manage Mirror Services form reappears.

8 Click on the Close button to close the Manage Mirror Services form.

Procedure 69-21 To delete a mirror service



Warning — Deleting a service may result in a service disruption for customers. Consider the implication of deleting the service before proceeding.

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 As required, configure the filter criteria to locate the service or range of services to be deleted. A list of services appears at the bottom of the Manage Mirror Services form.

3 Choose a mirror service or a range of services from the list.

4 Click on the Delete button. A warning form appears. This form is dynamic based on the priority of the service. Perform one of the following:

- **a** For services with a low priority, go to Step 5.
- **b** For services with a medium priority, configure the “Enter the highest priority of the service being deleted” text field by typing: Medium. Go to Step 5.
- **c** For services with a high priority, configure the “Enter the highest priority of the service being deleted” text field by typing: High. Go to step 5.

5 For all services regardless of how their priority is configured, acknowledge the check box that prompts you confirm that you understand the implications of deleting the service.



Note — If you select multiple services with different priorities, you must enter the highest priority level of selected services before you can delete the services.

6 Click on the Yes button to confirm the action. The service is deleted and removed from the list.

7 Click on the Close button to close the Manage Mirror Services form.

70 — IES management

70.1 IES management overview *70-2*

70.2 Sample IES configuration *70-8*

70.3 Workflow to create an IES *70-10*

70.4 IES management procedures *70-13*

70.1 IES management overview

An IES is a routed connectivity service in which the customer traffic passes through an L3 IP router interface to the Internet.

IES allows customer-facing IP interfaces in the same routing instance to be used for service network core-routing connectivity. IES requires that the IP addressing scheme that is used by the customer be unique among other provider addressing schemes and potentially the entire Internet.

Packets that arrive at the edge device are associated with an IES based on the access interface on which they arrive. An access interface is uniquely identified using:

- port
- service ID
- IP address

IES configuration

The 5620 SAM supports end-to-end IES configuration using the following methods:

- Tabbed configuration forms with an embedded navigation tree. The navigation tree provides a logical view of the service and acts as a configuration interface.
- Preconfigured template. A user who is assigned the template management role can create a service template. See "Managing templates" in the *5620 SAM Scripts and Templates Developer Guide* for more information about the administrative tasks associated with service templates.

The 5620 SAM supports the configuration in IES of an L3 aggregation mechanism called routed CO. Routed CO uses DHCP relay to manage dynamic subscriber hosts; the network resources for static subscriber hosts are explicitly provisioned. Routed CO supports all residential subscriber management functions of the 5620 SAM. See chapter 65 for more information about residential subscriber management and routed CO.

Routed CO uses a subscriber interface that defines up to 256 subnets. A subscriber interface has child objects called group interfaces. A group interface supports the configuration of multiple SAPs as child objects. A SAP in a group interface supports all residential subscriber management functions. A group interface does not allow the specification of IP subnets or addresses, but inherits the addressing scheme of the parent subscriber interface. The 5620 SAM service topology map displays IES subscriber interfaces, group interfaces, and the associated SAPs.

You can configure NAT for dynamic subscriber hosts in a routed CO deployment. NAT implementation in an IES requires a NAT configuration on the NE base routing instance and a NAT policy that is associated with a subscriber profile. See chapter 22 for information about configuring and deploying NAT on a base routing instance. See chapter 57 for information about configuring a NAT policy. See chapter 65 for information about associating a NAT policy with a subscriber profile.

When you use the 5620 SAM to create or discover a service, the 5620 SAM assigns a default Service Tier value to the service. The Service Tier parameter value is relevant only in the context of composite service topology views. See chapter 74 for more information about the hierarchical organization of composite services.

Common to all device services, such as IES, are policies that are assigned to the service. Policies are defined at a global level and can then be applied to components of the service, such as interfaces or circuits, when the service is configured or modified. The following policies are common to all device services:

- QoS policies define ingress classification, policing, shaping, and marking on the ingress side of the interface. QoS policies are configured using the Access Ingress Policy form, the Access Egress Policy form, and the ATM QoS Policy form.
- Policer control policies to control access ingress policers and access egress policers under a common hierarchy. Policer control policies are configured using the Policer Control Policy Manager.
- Scheduling policies define hierarchical rate limiting and scheduling to govern the scheduling of queues. Scheduler policies are configured using the Scheduler Policy form.
- Port scheduler policies define hierarchical bandwidth allocation and scheduling at the egress port level. Port scheduler policies are configured using the Port Scheduler Policy form.
- Filter policies control network traffic into or out of an interface or circuit based on DHCP, IP, or MAC matching criteria. Filter policies are configured using the ACL IP Filter form, the ACL MAC Filter form, and the DHCP Filter form.
- Accounting policies measure the traffic on a service to ensure proper billing and enforcement of SLAs. Accounting policies are configured using the Accounting Policy form.
- ANCP policies provide status and control information based on port-up and port-down messages and current line rate changes between the edge device and the access NE. ANCP policies are configured using the Manage Subscriber Policies form.
- Routing policies control the size and content of the routing tables, the routes that are advertised, and the best route to take to reach a destination. Routing policies are configured using the Routing Policy Manager.
- Time of day suites specify time and day restriction policies that are assigned to QoS policies and schedulers, ACL filters, and aggregation schedulers. Time of day suites and time range policies are configured using the Time of Day Suite form and Time Range form, respectively.

See chapter 42 for more information about policies.

Although IES is part of the routing domain, the usable IP address space may be limited. IES allows a portion of the service provider address space to be reserved for service IP provisioning and to be administered by a separate, but subordinate, address authority.

Multiple IESs can be created to separate customer-owned IP interfaces. More than one IES can be created for one customer. More than one IP interface can be created in one IES. All IP interfaces created in an IES belong to the same customer.

The IES IP interfaces are restricted to the routing protocols that can be defined on the interface based on the fact that the customer has a different routing domain for this service. The IP interfaces support the following routing protocols:

- RIP
- OSPF

- BGP
- IS-IS
- PIM
- IGMP

Customer routes can be advertised to the network core using static routes, RIP, or BGP. BGP and static routes are the most commonly used routing methods.

IPCP extensions allow you to configure IP addresses and DNS names of remote devices to enable inter-operability with other networks. Specifically setting an IPCP extension is necessary to connect to a mobile service provider network. Routers for mobile services rely on other network routers to provide IP addresses and DNS names (primary and secondary) for a PPP link.

When an IPCP extension is configured, an edge device configured with PPP/MLPPP can signal a far end device.

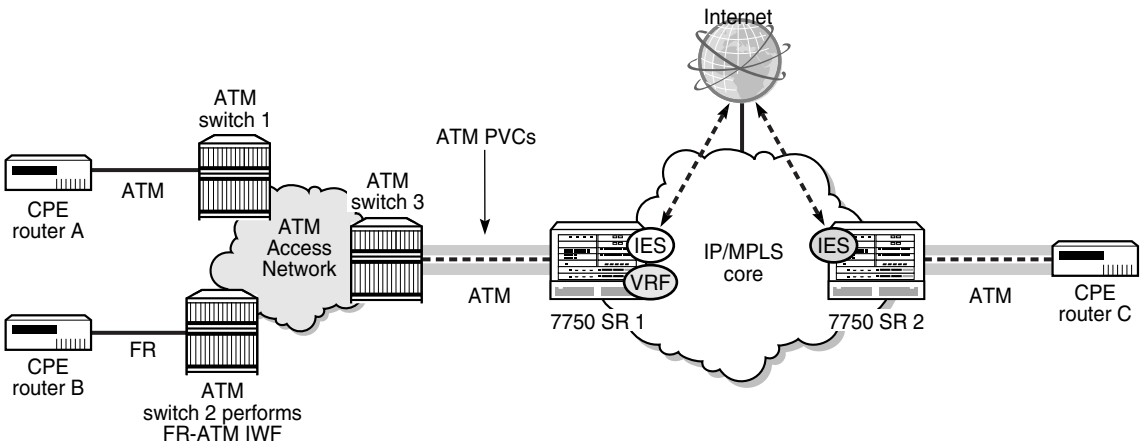
An IES can be connected to a VLL service or to a VPLS by an internal cross-connect through a CCAG adapter. This configuration eliminates the need for the physical port, cable, and other MDA-specific components and results in a less costly and more reliable interconnection. See chapter 74 for information about joining services to form composite services.

ATM SAP terminations for IES

CE routers that have access to an ATM network can connect with an IES service using ATM SAP terminations on a 7750 SR or 7710 SR. The interconnection between ATM point-to-point and L3 services uses RFC 2684-encapsulated IPv4 traffic over an ATM PVC that terminates on a specially configured SAP. All RFC 2684-encapsulated traffic can be routed over ATM networks, frame relay, and directly through ATM connections.

Figure 70-1 shows how CPE router A in an existing ATM network can access L3 IP services, such as an IES, using a statically configured ATM PVC on a 7750 SR (SR #1). CPE router B is connected to a frame relay, which connects to ATM switch 2 through IWF (service interworking). The RFC 2684-encapsulated traffic moves from both CPE routers through the ATM access network to a SAP configured on a 7750 SR #1 to serve a specific IES. At the same time, SDPs on the router are configured to a service to forward traffic over the IP/MPLS core. Destination CPE router C can receive RFC 2684-encapsulated traffic over an IP network over an ATM switch connected directly using 7750 SR #2.

Figure 70-1 ATM SAP network connection to an IES

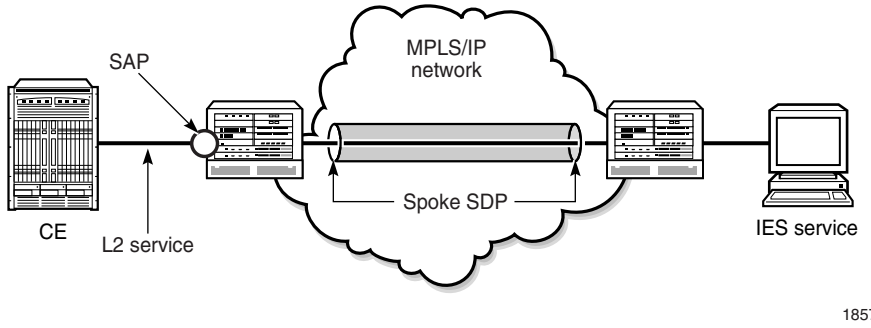


The two connection methods used between an ATM network and the IES router: LLC/SNAP encapsulation and VC multiplexing.

A VLL Epipe service can terminate directly on an IES service using an SDP spoke on the 7750 SR, 7450 ESS, or 7950 XRS. Traffic that terminates on an IES service is identified by the interface ID of the SDP on the L2 access router and the VC ID label in the service packet. All routing protocols supported by IES are also supported for spoke SDP termination.

Figure 70-2 shows a spoke SDP terminating directly on an IES. The spoke SDP could be tied to VLL Epipe or VPLS. No configuration is required for the CE-to-PE connection on the SAP.

Figure 70-2 SDP spoke termination on an L2 service



Routed CO dual homing using SRRP

Subscriber Router Redundancy Protocol (SRRP) allows two separate connections to an access NE such as DSLAM to operate in an active/standby configuration similar to the way in which VRRP interfaces operate. SRRP is a collection of functions and messaging protocols that allows a system to create a set of redundant gateway IP addresses that are shared by a local and remote NE.

Each SRRP instance is created within the context of a subscriber group IP interface and is identified by a unique SRRP instance ID, which must be unique within the NE. This SRRP instance controls the redundant routing for all subscriber subnets configured or associated with the group interface. One SRRP instance is supported for each group interface and the SRRP ID must be the same as the SRRP instance ID on the group IP interface on the redundant NE.

A subscriber subnet redundant gateway IP host address is assigned at the subscriber IP interface level and is used for each SRRP instance associated with the subscriber subnet. The redundant IP host address must be configured for a subscriber subnet before it can be associated with an SRRP instance.

When SRRP is active on a group interface, the SRRP instance advertises to a remote NE using in-band messaging on the group-interface SAPs and out-of-band messaging on the group-interface redundant interface. If the remote NE uses the same SRRP instance ID, one NE enters a master state, while the other NE enters a backup state. Since the NEs share a common SRRP gateway MAC address (used for the SRRP gateway IP address and for proxy ARP functions), either NE can act as the default gateway for the attached subscriber hosts. This functionality helps to preserve subscriber QoS enforcement. The master state allows routing to and from the subscriber hosts associated with the group IP interface. The backup state stops ingress forwarding for packets destined to the SRRP gateway MAC and causes all packets destined to subscriber hosts on the group IP interface to be forwarded to a redundant IP interface associated with the group IP interface.

Normally, when anti-spoofing is enabled on a group-interface SAP, the SAP drops SRRP packets because they do not contain a subscriber MAC or IP address. However, you can use a configuration option to enable anti-spoofing for subscriber hosts on a group-interface SAP that participates in SRRP advertisements.

The underlying mechanism that controls state transitions is based on a dynamic priority level that an SRRP instance maintains. The SRRP instance with the highest priority level assumes the master operating state. An SRRP instance with a higher current priority level always preempts an SRRP instance with a lower priority level. If the priority levels are equal, the SRRP instance with the lowest source SRRP host IP address assumes the master state. The local SRRP instance priority may also be controlled by associating the instance with an existing VRRP policy.

To prevent a flood of AccessInterfaceDown alarms that an SRRP fault or link failure may generate for LAG-based MSAPs, the 5620 SAM performs alarm suppression. See chapter 65 for more information.

The redundant IP interface is a special interface that connects two systems with one or more common SRRP instances. The interface is configured with a /31 address and a spoke SDP binding, creating an Ethernet pseudowire shortcut between the redundant NEs. When the SRRP instance is in backup state, the group interface associated with this instance is not allowed to forward or route traffic downstream towards the subscriber. As a result of this, the packets are shunted across the redundant interface so that the active group interface does the forwarding or routing.

If the redundant IP interface goes down, the system allows the group IP interfaces associated with the down interface to forward locally downstream, when they are in the backup SRRP state. While forwarding downstream in the backup state, the system uses the MAC address associated with the group IP interface, not the SRRP redundant gateway MAC address.

SRRP is supported on the 7450 ESS in mixed mode, 7710 SR and 7750 SR.

DoS protection

To protect an IES from a high incoming packet rate that characterizes a DoS attack, you can use the 5620 SAM to create DoS protection policies for the IES L3 access interfaces. A DoS protection policy limits the number of control-plane packets that an interface receives each second, and optionally logs a violation notification if a policy limit is exceeded. You can use the NE System Security form to view the violations for a specific NE.

You can configure a DoS protection policy to control the following on an IES L3 access interface:

- the control-plane packet arrival rate per subscriber host on the interface
- the overall control-plane packet arrival rate for the interface
- whether an NE sends a notification trap if a policy limit is exceeded

Each IES L3 access interface on an NE that supports DoS protection is automatically assigned a default DoS protection policy. This default policy limits only the overall packet arrival rate for the interface, and cannot be deleted or modified. See "To configure an NE DoS protection policy" in the *5620 SAM System Administrator Guide* for information about creating a DoS protection policy.

DDoS protection

To protect an IES from a high incoming packet rate that characterizes a DDoS attack, you can use the 5620 SAM to configure TMS interfaces to route malicious traffic through the ISA-TMS MDA where the malicious traffic is cleaned before being released to the network.

The TMS interface on an IES consists of one IES and two VPRNs as follows:

- The management VPRN communicates with the TMS server to determine whether incoming packets are malicious. Configuration of this VPRN is optional.
- The Off-Ramp VPRN receives the malicious traffic and routes it through the ISA-TMS MDA where the traffic is scrubbed. Configuration of this VPRN is mandatory.
- The On-Ramp IES returns the cleaned traffic to the network. Configuration of this IES is mandatory.

See Procedure 70-14 for information about creating a TMS interface on an IES.

You can configure a DDoS protection policy on an IES group interface SAP or L3 access interface. See "To configure an NE DDoS protection policy" in the *5620 SAM System Administrator Guide* for information about configuring a DDoS protection policy.

Local DHCP servers

A local DHCP server can be associated with a network interface or L3 access interface on an IES. See section 65.4.

Local user database

A local user database can be associated with a local DHCP server and PPPoE configurations on group interfaces. See section 65.4.

PPPoE protocol on IES

An IES can be configured to support PPPoE. PPPoE is used in subscriber networks to encapsulate PPP frames inside Ethernet frames. PPPoE combines the point-to-point protocol used by DSL sessions with Ethernet framing to support multiple subscribers in a LAN. Using the group interface configuration form, you can assign a PPPoE policy and a local user database to authenticate PPPoE subscribers.

L2TP configuration for IES

An IES group interface can be configured to terminate LNS PPP sessions. L2TP is a session-layer protocol that extends the PPP model by allowing L2 and PPP endpoints to reside on different devices that are interconnected by a PSN. L2TP extends the PPP sessions between the CPE and PPP/L2TP termination points on the L2TP network server (LNS), via an intermediate L2TP access concentrator (LAC). The LAC is the initiator of session-generated L2TP tunnels; the LNS is the server that waits for new tunnels. Manually configured and initiated L2TP tunnels can be initiated or stopped from either the LNS or LAC.

After a tunnel is established, the network traffic between the peers is bidirectional. If a tunnel carrying a session fails, another tunnel from the same tunnel group re-establishes the session. Within each L2TP tunnel, one or more L2TP sessions can exist. Each L2TP session transports PPP packets.

At least one ISA-LNS group must be configured for the LNS NE.

On an LNS NE, L2TP destinations configured for L2TP tunnel profiles can include the following:

- loopback L3 access interfaces for a VPRN or IES service
- loopback interfaces configured for a base routing instance

See chapter 14 for more information about ISA-LNS groups. See Procedure 14-6 for information about creating and configuring an ISA-LNS group. See chapter 23 for more information about L2TP. See Procedure 70-12 for information about configuring an IES group interface to terminate LNS PPP sessions.

70.2 Sample IES configuration

Figure 70-3 shows a sample IES configuration.

Figure 70-3 Sample IES configuration

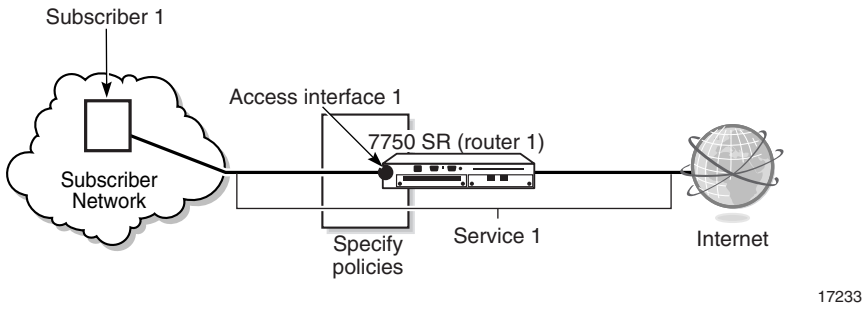


Table 70-1 lists the high-level tasks necessary to configure this sample IES.

Table 70-1 Sample IES configuration

Task	Description
1. Configure policies as required	Policies should be configured prior to creating a service. Participation in policies by access interfaces is defined when you configure or modify access interfaces during service creation or modification. The following key policies can be applied to resources that are part of an IES. • QoS access ingress and egress interface policies. Choose Policies→QoS→SROS QoS→Access Ingress or Access Egress, then the name of the form you need to configure, to open these forms. • Scheduler policy. Choose Policies→QoS→SROS QoS→Scheduler, then the name of the form you need to configure, to open the scheduler policy forms. • ACL IP filter policies. Choose Policies→Filter→ACL IP Filter to open the IP filter form. • Accounting policy. Choose Tools→Statistics→Accounting Policies to open the accounting policy form. • ANCP policy. Choose Policies→Residential Subscriber to open the Manage Subscriber Policies form.
2. Create and configure Subscriber 1	Choose Manage→Service→Customers to open the customer manager form and create a customer.

(1 of 2)

Task	Description

3. Create and configure Service 1	Ensure that the operator creating the service has Service Mgmt and Interface Mgmt user group privileges. See "5620 SAM user security tasks" in the *5620 SAM System Administrator Guide* for more information about user and user group privileges.
	Choose Create→Service→IES. Use the tabbed form and embedded navigation tree to configure the service. You configure the following key elements when you configure Service 1.
	• Choose Subscriber 1 as the customer for the IES.
	• Choose router 1 as the site for the IES.
	• Create and configure Access interface 1. You do the following to configure an access interface:
	  • Configure general parameters such as a name, ID, and MAC address.
	  • Assign an application profile, if required.
	  • Assign a transit IP or transit prefix policy, if required.
	  • Specify a port that is in access or hybrid mode.
	  • Add unicast routing protocols as required.
	  • Assign ingress and egress QoS policies, as required.
	  • Add multicast routing protocols as required.
	  • Assign an aggregation scheduler for traffic rate limiting across the card or port, if required. Otherwise, assign ingress and egress scheduler policies.
	  • Assign ACL filter policies as required.
	  • Assign an accounting policy, if required.
	  • Specify a local DHCP server, if required.
	  • Specify a ToD suite, if required.
	  • Configure subscriber management parameters, if required.
	  • Specify a DoS protection policy, if required.
	  • Specify a DDoS protection policy, if required.
	  • Specify one or more IP addresses for the IES access interface: one primary IP address and, optionally, multiple secondary IP addresses.
	  • Specify BFD parameters as required.
	  • Configure the ARP timeout and proxy ARP settings, if required.
	  • Configure IPCP parameters, if required.
	  • Configure ICMP parameters, if required.
	  • Configure DHCP parameters, if required.
	  • Configure ARP host configuration, if required.
	  • Configure VRRP parameters, if required.
	  • Configure anti-spoofing parameters, if required.
	  • Create a MEP, if required.
	  • Configure router advertisement parameters.
	  • Create QoS policy overrides, if required.
	  • Configure ANCP parameters, if required.

(2 of 2)

70.3 Workflow to create an IES

The following workflow lists the high-level steps required to create an IES. As a prerequisite for creating a IES, this workflow assumes the following:

- a group or customer with the required user access privileges has been configured.
- the IP or IP/MPLS core network exists.
- any required service tunnels are created including the static or dynamic LSP required to create the service tunnel; see Procedure 27-1.
- the access ports for the service are created; see chapter 16 for more information.

- any required pre-defined routing, QoS, scheduling, filter, accounting, and time of day suite policies are created; see chapter 42 for more information. You do not have to create pre-defined policies if policies are created on a per-service basis.
- any required MP-BGP for PE-to-PE routing is configured; see chapter 23 for more information about protocol configuration.

1 Create the IES. See Procedure 70-1.

   i Choose a customer to associate with the IES.

   ii Define the general properties for the IES.

   iii Turn up the IES service.

2 As required, configure AA reporting to the 5670 RAM. See Procedure 70-2.

3 As required, create an IES site or GNE IES site. See Procedures 70-3 and 70-4.

4 As required, perform one or more of the following on an IES site.

   a Apply routing protocols, such as OSPF, RIP, or IS-IS, to an IES site, if required. See Procedure 70-5.

   b Add an IGMP interface to an IES. See Procedure 70-6.

   c Add a PIM interface to an IES. See Procedure 70-7.

   d Create an L2 SDP spoke termination on an IES service. See Procedure 70-8.

   e Add a subscriber interface to an IES. See Procedure 70-10.

   f Add an AARP interface to an IES. See Procedure 70-11.

   g Add a group interface to an IES. See Procedure 70-12.

   h Configure WLAN GW for an IES group interface. See Procedure 70-13.

   i Add a TMS interface to the IES. See Procedure 70-14.

   j Implement dual homing using SRR. See Procedure 70-15.

   k Create and enable a video interface for the IES site, if required. See Procedure 30-2.

5 As required, create an L3 access interface on an IES site. See Procedure 70-17.

6 As required, perform one or more of the following on an IES L3 access interface.

   a Configure custom object attributes for AA reporting to the 5670 RAM. See Procedure 70-18.

   b Bind the L3 access interface to a VPLS site. See Procedure 70-19.

   c Apply OSPF, RIP, or IS-IS to an IES L3 interface. See Procedure 70-20.

   d Assign ingress and egress QoS policies. See Procedure 70-21.

   e Assign ingress and egress QoS policies on the 7210 SAS. See Procedure 70-22.

f Configure scheduling. See Procedure 70-23.

g Assign ingress and egress ACL filters. See Procedure 70-24.

h Associate a local DHCPv4 or DCHPv6 server. See Procedure 70-25.

i Assign an accounting policy. See Procedure 70-26.

j Assign an ANCP policy. See Procedure 70-27.

k Assign a time of day suite. See Procedure 70-28.

l Configure residential subscriber management. See Procedure 70-29.

m Assign a DoS protection policy or DDoS protection policy. See Procedure 70-30.

n Assign an IP address. See Procedure 70-31.

o Configure bi-directional forwarding detection. See Procedure 70-32.

p Configure IPv4 ICMP. See Procedure 70-33.

q Configure IPv6 ICMP. See Procedure 70-34.

r Configure IPCP. See Procedure 70-35.

s Configure ARP. See Procedure 70-36.

t Configure neighbor discovery. See Procedure 70-37.

u Configure IPv4 DHCP. See Procedure 70-38.

v Configure ATM. See Procedure 70-39.

w Create a VRRP instance. See Procedure 70-40.

x Configure anti-spoofing filters. See Procedure 70-41.

y Configure router advertisement. See Procedure 70-42.

z Specify queue overrides. See Procedure 70-43.

aa Configure IPv6 DHCP. See Procedure 70-44.

ab Configure an MLD interface on the L3 access interface. See Procedure 23-62.

7 As required, view IES information.

a View the IES service operational status. See Procedure 70-45.

b View the service topology map associated with an IES. See Procedure 70-46.

8 As required, create an L3 access interface on an IES site.

9 As required, modify a IES.

a Using the Manage Services form. See Procedure 70-47.

b Using the topology view. See Procedure 70-48.

10 As required, delete an IES. See Procedure 70-49.

70.4 IES management procedures

Use the following procedures to perform IES creation and management tasks.

Procedure 70-1 To create an IES



Note — The 7210 SAS-M does not support IES in Network mode.

1 Choose Create→Service→IES from the 5620 SAM main menu. The IES Service (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the IES. The Select Customer - IES Service form opens.

3 Choose a customer for the IES and click on the OK button. The Select Customer - IES Service form closes, and the IES Service (Create) form reappears with the customer information displayed in the Customer panel.

4 Configure the parameters:

- Service ID
- Auto-Assign ID
- SVC Mgr Service ID
- Service Name
- Description
- Service Tier
- Service Priority
- Administrative State
- Current OLC State
- Revert OLC State

The Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.

The SVC Mgr Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.

The Current OLC State and Revert OLC State parameters are configurable when you click on the Apply button.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button to confirm the action. The IES Service (Create) form closes.

7 Close the Manage Services form.

Procedure 70-2 To configure an IES for AA reporting to the 5670 RAM

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services is displayed.

3 Choose an IES in the list and click on the Properties button. The IES Service (Edit) form opens with the General tab displayed.

4 Click on the Application Assurance tab. The 5670 RAM Parameters tab is displayed.

5 Configure the parameters:

- Enable Application Performance Reporting
- Report Customer Name
- Number of IP Detail Addresses

6 To configure one or more custom DCP groups, see the custom DCP group configuration procedure in chapter 76.

7 To specify an application or application group for IP detail reporting, click on the IP Detail Application or IP Detail Application Group tab, as required. The IP Detail Application or IP Detail Application Group (Create) form opens.

Otherwise, go to step 13.

8 Configure the parameters:

- ID
- Auto-Assign ID

9 Click on the Select button and choose an application or application group from the Select Application or Select Application Group form.

10 Click on the OK button. The IP Detail Application or IP Detail Application Group (Create) form closes, and a dialog box appears.

11 Click on the OK button. The application or application group is listed on the IES Service (Create) form.

12 To specify another application or application group for IP detail reporting, repeat steps 7 to 11.



Note — You can specify up to 10 applications and up to 10 application groups.

13 Close the IES Service (Edit) form.

14 Close the Manage Services form.

Procedure 70-3 To configure an IES site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Perform one of the following.

a Create an IES site by performing the following steps:

i On the navigation tree, right-click on the Site icon and choose Create IES Site. The Select Network Elements - IES Service form opens with a list of available sites displayed.

ii Choose a site and click on the OK button. The IES Site (Create) form opens with the General tab displayed.

b Configure an existing IES site by performing the following steps:

i Expand the Sites icon in the service navigation tree.

ii Right-click on a Site icon and choose Properties from the contextual menu. The IES Site (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State
- Tunnel Fault Notification

Tunnel Fault Notification is configurable on sites where the device has ports configured in access or hybrid mode with QinQ encapsulation.

If you are configuring a tunnel facility MEP, Tunnel Fault Notification must be set to Accept in order to receive the fault notification from the tunnel facility MEP.

6 Click on the OK button. A dialog box appears.

7 Click on the OK button. The IES Site (Create) form closes, and the IES Service (Edit) form reappears with the new site information displayed in the service navigation tree.

8 Close the IES Service (Edit) form.

9 Close the Manage Services form.

Procedure 70-4 To configure a GNE site on an IES service

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES service and click on the Properties button. The IES Service (Edit) form opens with the General tab displayed.

4 On the component tree, right-click on IES Service and choose Create GNE Site. The Select Network Elements - IES Service form opens with a list of available sites.

5 Choose a site and click on the OK button. The GNE Site (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Name
- Description

7 Click on the Apply button.

8 To configure an interface for the GNE site, perform the following steps:

i Click on the GNE Service Interfaces tab and then click on the Create button. The GNE Service Interface (Create) form opens with the general tab displayed.

ii Configure the parameters:

- Name
- Description
- Type

iii Click on the Ports tab and then click on the Select button beside the Interface Index field. The Select Generic NE Interface form appears.

iv Choose an interface and click on the OK button. The GNE Service Interface (Create) form reappears with the interface information displayed.

v Configure the parameters:

- Encapsulation Type
- Outer Encapsulation Value
- Inner Encapsulation Value

vi Click on the OK button. The GNE Site (Create) form reappears with the interface information displayed in the service component tree.

9 Click on the Scripts tab to attach or execute configuration scripts on the GNE site.

The Scripts tab displays the script instances and versions that are applied to the device. See "Script management" in the *5620 SAM Scripts and Templates Developer Guide* for more information.

10 Click on the OK button. The IES Service (Edit) form reappears with the new information displayed in the service component tree.

11 Click on the OK button. The IES Service (Edit) form closes.

You can use the topology maps to view the service. See chapter 6 for more information about service topology maps.

Procedure 70-5 To apply OSPF, RIP, or IS-IS to an IES site



Note — OSPF, RIP, or IS-IS must be enabled at the routing instance level before you can apply OSPF, RIP, or IS-IS to an IES.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose an IES in the list and click on the Properties button. The IES Site (Edit) form opens with the general properties of the service displayed on the General tab.

4 Click on the Sites tab.

5 Choose a site in the list and click on the Properties button. The IES Site (Edit) form opens.

6 Click on the Routing tab.

7 In the Protocols tab, click on the Create button. The Create Interface form opens.

8 Specify the interface type by configuring the What type of interface would you like to create? parameter.

9 Click on the OK button. The Interface (Create) form opens. See section 23.2 for information about configuring specific routing protocols.

Procedure 70-6 To add an IGMP interface to an IES



Note — IGMP must be enabled on the NE routing instance before you can create an IGMP interface.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose an IES and click on the Properties button. The IES Service (Edit) form opens with the General tab displayed.

4 Expand the Sites icon in the service navigation tree.

5 Right-click on the Site icon and choose Properties from the contextual menu. The IES Site (Edit) form opens with the General tab displayed.

6 Click on the Multicast tab.

7 Click on the Interfaces tab.

8 Click on the Add button. The Create Interface form opens.

9 Set the What type of interface would you like to create? parameter to IGMP.

10 Click on the OK button. The IGMP Interface (Create) form opens with the General tab displayed.

11 Click on the Select button to specify an interface. The Select Interface form opens.

12 Click the Search button. A list of interfaces appears at the bottom of the Select Interface form.

13 Choose an interface and click the OK button. The Select Interface form closes and the Interface panel refreshes with the interface parameters.

14 Configure the parameters:

- Description
- Administrative State
- Administrative Version

15 Click on the Behavior tab.

16 Configure the parameters:

- Import Policy
- Maximum Number of Groups
- Maximum Number of Sources
- Subnet Check
- Disable Router Alert Check
- Sub Hosts Only

17 Click on the Multicast CAC tab to add a multicast CAC policy, if required. The General tab is displayed.

18 Click on the Select button in the Select Multicast CAC Policy panel to choose a multicast CAC policy. The Select Multicast CAC Policy - IGMP Interface form opens.

19 Choose a multicast CAC policy and click on the OK button. The Select Multicast CAC Policy - IGMP Interface form closes and the IGMP Interface, Routing Instance (Create) form appears.

20 Configure the parameters:

- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)
- Constraint Admin State

21 Click on the Static Group/Source tab to add a static multicast group or source, if required.

22 Click on the Create button to add a new entry. The StaticGrpSrc, Interface ID - 6, Routing Instance (Create) form opens.

23 Configure the parameters:

- Static Multicast Group
- Static Source

24 Click on the OK button. The StaticGrpSrc, Routing Instance (Create) form closes and a dialog box appears.

25 Click on the OK button to confirm the action. The IGMP Interface, Routing Instance (Create) form reappears.

26 Click on the OK button to close the IGMP Interface, Routing Instance (Create) form.

27 Click on the OK button to close the IGMP Interface (Create) form.

28 Click on the Group Interfaces tab to identify an IGMP group interface for the IES service, if required.

i Click on the Create button. The IGMP Group Interface - Routing Instance (Create) form opens with the General tab displayed.

ii Configure the parameters:

- Description
- Query Source IP
- Administrative State
- Administrative Version
- Forwarding Service ID

iii Click on the Select button beside the Interface ID field in the IGMP Group Interface panel to choose an IGMP group interface.

iv Choose an IGMP group interface and click on the OK button. The Select IGMP Group Interface form closes and the IGMP Group Interface - Routing Instance (Create) form appears.

v Configure the parameters:

- Maximum Number of Groups
- Maximum Number of Sources

vi Click on the Multicast CAC tab to add a multicast CAC policy, if required. The General tab is displayed.

vii Click on the Select button in the Multicast CAC Policy panel. The Select Multicast CAC Policy - IGMP Interface Group form opens.

viii Choose a multicast CAC policy and click on the OK button. The Select Multicast CAC Policy - IGMP Group Interface form closes and the IGMP Interface, Routing Instance (Create) form reappears.

ix Configure the parameters:

- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)
- Constraint Admin State

x Click on the OK button to close the IGMP Group Interface - Routing Instance (Create) form.

29 Close the Site (Edit) form.

30 Close the IES Service (Edit) form.

31 Close the Manage Services form.

Procedure 70-7 To add a PIM interface to an IES



Note — Before you can add a PIM interface to an IES, PIM must be applied to All or IES during the PIM configuration at the routing instance level. See Procedure 23-40 for more information.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose an IES and click on the Properties button. The IES Service (Edit) form opens with the General tab displayed.

4 Expand the Sites icon in the service navigation tree.

5 Right-click on the Site icon and choose Properties from the contextual menu. The IES Site (Edit) form opens with the General tab displayed.

6 Click on the Multicast tab.

7 Click on the Add button. The Create Interface form opens.

8 Set the What type of interface would you like to create? parameter to PIM.

9 Click on the OK button. The PIM Interface (Create) form opens with the General tab displayed.

10 Click on the Select button to specify an interface. The Select Interface - PIM Interface form opens.

11 Configure the filter criteria. A list of available L3 access interfaces appears at the bottom of the Select Interface - PIM Interface form.

12 Choose an interface and click on the OK button. The Select Interface - PIM Interface form closes and the PIM Interface, Routing Instance (Create) form refreshes with the L3 access interface information.

13 Configure the parameters:

- Description
- Administrative State
- Administrative State IPv4
- BFD Enabled
- IPv6 BFD Enabled

14 Click on the Behavior tab.

15 Configure the parameters:

- Hello Interval (seconds)
- Tracking Support
- BSM Check Router Alert
- Improved assert
- Max Groups
- Three Way Hello
- Multicast Senders
- Hello Multiplier
- Assert Period
- DR Priority
- Sticky DR
- Sticky DR Priority
- P2MP to LDP Tree Join Enabled



Note — The Sticky DR Priority parameter is configurable when the Sticky DR parameter is enabled.

16 Click on the Neighbor tab, if present, to view and edit information. The Neighbor tab is present only when a neighbor PIM interface exists.

17 Click on the Multicast CAC tab to add a multicast CAC policy, if required. The General tab is displayed.

18 Click on the Select button in the Multicast CAC Policy panel to choose a multicast CAC policy. The Select Multicast CAC Policy - PIM Interface form opens.

19 Choose a multicast CAC policy and click on the OK button. The Select Multicast CAC Policy - PIM Interface form closes and the PIM Interface, Routing Instance (Create) form reappears.

20 Configure the parameters:

- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)
- Constraint Admin State

21 Click on the IPv6 Specifics tab.

22 Configure the IPv6 Administrative State parameter.

23 Close the PIM Interface (Create) form.

24 Close the IES Site (Edit) form.

25 Close the IES Service (Edit) form.

26 Close the Manage Services form.

Procedure 70-8 To create an L2 SDP spoke termination on an IES service

Ensure that a service and site are created in the IES. To terminate an L2 service on an IES SDP spoke, you must identify the VC and an interface that belong to the VC. The interface must not have an associated port.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose an IES and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 On the navigation tree, click on the site to which you need to add the L2 SDP spoke termination; expand the entries for that site.

5 Right-click on Spoke Sdp Bindings and choose Create Spoke SDP Binding. The Spoke SDP Binding (Create) form opens with the General tab displayed.

6 Specify a source interface for the spoke SDP binding.

i Click on the Select button in the Source Interface panel. The Select Source Interface - Spoke SDP Binding form opens.

ii Configure the filter criteria. A list of source interfaces appears at the bottom of the Select Source Interface - Spoke SDP Binding form.

iii Choose a source interface and click on the OK button. The Select Source Interface - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form appears.

7 Specify a destination NE for the spoke SDP binding:

a If the destination NE is a managed NE, choose from a list of managed NEs.

i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element form opens.

ii Choose a destination NE and click on the OK button. The Select Destination Network Element form closes, and the Spoke SDP Binding (Create) form refreshes with the tunnel termination site (the destination NE) identifier displayed.

b If the destination NE is an unmanaged NE, specify the system ID for the Tunnel Termination Site parameter.

8 Configure the parameters:

- Description
- VC ID
- VC Type
- Auto-Assign ID
- Ingress Label
- Egress Label
- Enable Ingress FlowSpec IPv4
- Enable Ingress FlowSpec IPv6

These parameters appear only when a source interface is assigned to the spoke SDP binding.

9 Configure the parameters in the Hash Label panel:

- Enable Hash Label
- Enable Signal Capability

The Enable Hash Label and Enable Signal Capability parameters can only be configured for spoke-SDP bindings that are access interface terminated.

10 Perform one of the following to specify a transport tunnel for the spoke SDP binding.

a Let the 5620 SAM configure the transport tunnel automatically.

i Enable the Auto-Select Transport Tunnel parameter.

ii Configure the Tunnel Auto-Selection Transport Preference parameter.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens.

ii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier.

c Configure an MPLS-TP transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens.

ii Select an MPLS-TP service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier. See Procedure 27-1 for more information about how to create an MPLS-TP service tunnel.

11 Specify an application profile for the spoke SDP binding.

i Click on the Select button beside the Application Profile parameter. The Application Profile String: - Spoke SDP Binding form opens.

ii Configure the filter criteria. A list of application profiles appears.

iii Choose an application profile and click on the OK button. The Application Profile String: - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form appears.



Note — The Application Profile String: - Spoke SDP Binding - IES service form displays only local profiles on the NE.

12 Choose one of the following AA transit policy types, if required.



Note 1 — You can only associate one AA transit policy type with a service object.

Note 2 — To bind a transit policy to an L3 access interface, a port must already exist on the interface.

Note 3 — You can bind a transit policy to only one L3 access interface or spoke SDP binding per NE.

Note 4 — The transit policy and the application profile must belong to the same application assurance group or partition.

a Associate an AA transit IP policy with the service object:

i Click on the Select button in the Transit IP Policy panel. The Select Transit IP Policy form opens.

ii Choose a transit IP policy and click on the OK button.

b Associate an AA transit prefix policy with the service object:

i Click on the Select button in the Transit Prefix Policy panel. The Select Transit Prefix Policy form opens.

ii Choose a transit IP policy and click on the OK button.

13 Associate an AA redundant protocol with the service object:

i Click on the Select button in the AA Redundant Protocol panel. The Select AA Redundant Protocol form opens.

ii Choose an AA redundant protocol and click on the OK button. The Select AA Redundant Protocol form closes.

14 Configure the AARP Service Reference Type parameter.

15 To configure custom object attributes for AA reporting to the 5670 RAM, perform the following steps:

i Click on the 5670 RAM Parameters tab.

ii Click on the Reporting tab.

iii Click on the Create button. The AA Reporting (Create) form opens.

iv Configure the parameters:

- Customer Name
- Subscriber Class
- Total Bandwidth Upstream (Kbps)
- Class of Service 1 Bandwidth Upstream (Kbps)
- Class of Service 2 Bandwidth Upstream (Kbps)
- Class of Service 3 Bandwidth Upstream (Kbps)
- Class of Service 4 Bandwidth Upstream (Kbps)
- Subscriber Name
- Subscriber Type
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)

v Click on the OK button. The AA Reporting (Create) form closes and the reporting object is displayed in the list.

vi Click on the General tab.

16 Click on the QoS tab.

17 Configure the required parameters in the Forwarding Plane Redirect panel:

i Click on the Network Policy Select button to assign a policy to the Spoke SDP Binding. The Select Network Policy form opens.

ii Choose a policy and click on the OK button. The Network Policy form closes and the Spoke SDP Binding (Create) form refreshes with the Network Policy information displayed.

iii Click on the Ingress Queue Group Template Policy Select button to assign a policy to the Spoke SDP Binding. The Select Ingress Queue Group Template Policy form opens.

iv Choose a policy and click on the OK button. The Ingress Queue Group Template Policy form closes and the Spoke SDP Binding (Create) form refreshes with the Ingress Queue Group Template Policy information displayed.

v Configure the Instance ID parameter.

18 Configure the required parameters in the Port Redirect panel:

i Click on the Network Policy Select button to assign a policy to the Spoke SDP Binding. The Select Network Policy form opens.

ii Choose a policy and click on the OK button. The Network Policy form closes and the Spoke SDP Binding (Create) form refreshes with the Network Policy information displayed.

iii Click on the Egress Queue Group Template Policy Select button to assign a policy to the Spoke SDP Binding. The Select Egress Queue Group Template Policy form opens.

iv Choose a policy and click on the OK button. The Egress Queue Group Template Policy form closes and the Spoke SDP Binding (Create) form refreshes with the Egress Queue Group Template Policy information displayed.

v Configure the Instance ID parameter.

19 Click on the States tab.

20 Configure the Administrative State parameter.

21 Assign ingress and egress ACL filters to the spoke SDP binding, if required.

i Click on the ACL tab.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - Spoke SDP Binding form opens.

iii Choose an ingress ACL filter and click on the OK button. The Select Ingress Filter - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form reappears with the ingress ACL filter information displayed.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - Spoke SDP Binding form opens.

v Choose an egress ACL filter and click on the OK button. The Select Egress Filter - Spoke SDP Binding form closes, and the L3 Access Interface (Create) form reappears with the egress ACL filter information displayed.

22 Assign an accounting policy to the spoke SDP binding, if required.

i Click on the Accounting tab.

ii Configure the Collect Accounting Statistics parameter.

iii Click on the Select button to choose an accounting policy. The Select Accounting Policy - Spoke SDP Binding form opens.

iv Choose an accounting policy and click on the OK button. The Select Accounting Policy - Spoke SDP Binding form closes, and the L3 Access Interface (Create) form reappears with the accounting policy information displayed.

23 Associate a MEP with an SDP binding, if required.

i Click on the MEPs tab.

ii Click on the Create button. The MEP (Create) form opens with the General tab displayed.

iii Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

iv Choose an entry and click on the OK button. The Select Maintenance Entity Group form closes.

v Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Propagation
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)
- CCM Padding Packet Size (Bytes)



Note — The CCM Padding Packet Size (Bytes) parameter cannot be configured when the CCM interval parameter is set to 10 ms or 100 ms.

vi If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab. Otherwise, go to step 24.

vii Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

viii Click on the AIS tab.

ix Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

24 Click on the OK button. The MEP (Create) form closes.

25 Click on the OK button. The Spoke SDP Binding (Create) form closes and a dialog box appears.

26 Click on the OK button. The IES Service (Edit) form reappears with the new information displayed in the service navigation tree.

Procedure 70-9 To configure an MPLS-TP static pseudowire on an IES spoke SDP binding

Perform this procedure to create an MPLS-TP static pseudowire on the spoke SDP binding. An MPLS-TP service tunnel must be used in the SDP binding, and the Control Word parameter for pseudowire OAM must be set to Preferred. See Procedure 70-8.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Select an IES and click on the Properties button. The IES Service (Edit) form opens.

4 On the navigation tree, expand the site on which you want to configure the spoke SDP binding, and expand the Spoke SDP Bindings icon.

5 Click on the SDP binding on which you want to configure the MPLS-TP static pseudowire. The Spoke SDP Binding (Edit) form opens with the General tab displayed.

6 Click on the Control Channel tab.

7 Configure the parameters:

- Status
- Refresh Timer (seconds)
- Request Timer (seconds)
- Retry Timer (seconds)
- Timeout Multiplier
- Acknowledged

8 Click on the MPLS-TP PW tab.

9 Click on the Create button. The PW Path ID (Create) form opens.

10 Configure the Path AGI parameter.

11 Configure the parameters in the Source Attachment Individual Identifier panel:

- SAII Global ID
- SAII Node ID
- SAII AC ID

12 Configure the parameters in the Target Attachment Individual Identifier panel:

- TAII Global ID
- TAII Node ID
- TAII AC ID

13 Click on the OK button. The PW Path ID (Create) form closes.

14 Click on the OK button. The Spoke SDP Binding (Edit) form closes.

15 Close the IES Service (Edit) form.

16 Close the Manage Services form.

Procedure 70-10 To configure a subscriber interface on an IES

The 7450 ESS in mixed mode, 7710 SR and 7750 SR support the configuration of a subscriber interface in an IES.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears at the bottom of the Manage Services form.

3 Choose an IES and click on the Properties button. The IES Service (Edit) form opens.

4 On the navigation tree, navigate to the Subscriber Interfaces object. Perform one of the following:

a To create a subscriber interface, right-click on the Subscriber Interfaces object and choose Create IES Subscriber Interface from the menu. The IES Subscriber Interface (Create) form opens.

b To modify a subscriber interface, right-click on the subscriber interface object and choose Properties from the menu. The IES Subscriber Interface (Edit) form opens.

5 Configure the parameters:

- Auto-Assign ID
- Interface ID
- Name
- Description
- Administrative State
- Default Primary DNS Server Address
- Default Secondary DNS Server Address
- Allow Unmatched Subnets
- Tunnel Fault Notification

The Tunnel Fault Notification parameter is configurable on interfaces where the device has ports configured in access or hybrid mode with QinQ encapsulation.

If you are configuring a tunnel facility MEP, Tunnel Fault Notification must be set to Accept, in order to receive the fault notification from the tunnel facility MEP.



Note 1 — The Name value for a subscriber interface must be unique in the NE.

Note 2 — You must configure the Default Primary DNS Server Address parameter before you can configure the Default Secondary DNS Server Address parameter.

6 Click on the Select button in the Forwarding Service panel to choose a service. The Select Forwarding Service - IES Subscriber Interface form opens.

7 Choose a service and click on the OK button. The Select Forwarding Service - IES Subscriber Interface form closes, and the IES Subscriber Interface (Create) form reappears with the service information displayed.

8 Click on the Select button in the Forwarding Subscriber Interface panel to choose a subscriber. The Select Forwarding Subscriber Interface - IES Subscriber Interface form opens.

9 Choose a subscriber and click on the OK button. The Select Forwarding Subscriber Interface - IES Subscriber Interface form closes, and the IES Subscriber Interface (Create) form reappears with the subscriber information displayed.

10 Configure IPv6 forwarding on the subscriber interface, if required.

i Configure the IPv6 Allowed parameter.

ii Configure the parameters.

- Admin Link Local Address
- IPv6 Delegated Prefix Length
- IPv6 Allow Unmatching Prefixes
- Default Primary IPv6 DNS Server Address
- Default Secondary IPv6 DNS Server Address

You must remove the check mark from the Default check box to access the Default Primary IPv6 DNS Server Address and Default Secondary IPv6 DNS Server Address parameters.

iii Click on the IPv6 Subscriber Prefixes tab.

iv Choose a subscriber prefix and click on the Properties button, or click on the Create button to create a new subscriber prefix.

v In the Subscriber Prefix [Edit|Create] form, configure the parameters:

- Address ID
- IP Address
- Prefix Length
- WAN Host
- Prefix Delegation

11 Configure the Interface Class parameters, if required.

i Configure the Class parameter.

ii If you selected a value of Unnumbered for the Class parameter, configure the Unnumbered Type parameter.

iii Configure the Interface Name parameter or the IP Address parameter.

12 Configure the DHCP Server Synchronization parameters, if required:

- Delayed Up Period
- Delay on Init Only

13 Create IP addresses for the subscriber interface that are inherited by the SAPs in the group interfaces that are child objects of the subscriber interface.

i Click on the Addresses tab.

ii Click on the Create button. The IP Address (Create) form opens.

iii Configure the parameters:

- Address ID
- IP Address
- Prefix Length
- Populate Host Routes
- Track SRRP Instance
- Hold Up Time (milliseconds)
- Gateway IP Address
- Broadcast Address Format

iv Click on the OK button. The IP Address (Create) form closes, and a dialog box appears.

v Click on the OK button. The IES Subscriber Interface (Create) form reappears with the assigned IP addresses displayed.

vi Repeat steps ii to v for each additional IP address that you need to create.

14 Click on the DHCP tab.

15 Configure the parameters:

- IP address
- Use as source
- Enable DHCP Relay
- Description

16 Click on the Server tab.

17 Configure the parameters.

- Server 1 through Server 8
- Administrative State
- Emulated Server IP Address
- Lease Time
- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time Override

The Number of Days, Number of Hours, Number of Minutes, Number of Seconds, and Lease Time Override parameters are configurable only when the Lease Time parameter is set to Specified Time Period.

18 Click on the Client Applications tab.

19 Configure the Client Applications parameter. You can enable either or both of the PPPoE or DHCP choices.

20 Click on the PPPoE tab.

21 Configure the parameters:

- Description
- Session Limit

22 Click on the OK button. The IES Subscriber Interface (Create) form closes, and a dialog box appears.

23 Click on the OK button. The IES Service (Edit) form reappears with the new subscriber interface displayed in the service navigation tree.

24 Click on the OK button. A dialog box appears.

25 Click on the Yes button. The IES Service (Edit) form closes, and the Manage Services form reappears.

26 Close the Manage Services form.

Procedure 70-11 To add an AARP interface to an IES

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears at the bottom of the Manage Services form.

3 Choose an IES and click on the Properties button. The IES Service Subscriber (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site to which you need to add the subscriber interface; expand the entries for that site.

5 Right-click on the AARP Interfaces icon below the site to which you need to add the subscriber interface, and choose Create AARP Interface. The AARP Interface (Create) form opens.

6 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- Configured IP MTU (Octets)

7 Click on the OK button. The AARP Interface (Create) form closes, and a dialog box appears.

8 Click on the OK button. The IES Service (Edit) form reappears with the new AARP interface displayed in the service navigation tree.

9 Click on the OK button. A dialog box appears.

10 Click on the Yes button. The IES Service (Edit) form closes, and the Manage Services form reappears.

11 Close the Manage Services form.

Procedure 70-12 To configure a group interface on an IES

The 7450 ESS in mixed mode, 7710 SR and 7750 SR support the configuration of a group interface in an IES.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose an IES and click on the Properties button. The IES Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, navigate to the site and subscriber interface on which you need to configure a group interface. Perform one of the following:

   a To create a group interface, right-click on the subscriber interface and choose Create IES Group Interface from the menu. The IES Group Interface (Create) form opens.

   b To modify a group interface, right-click on the group interface object and choose Properties from the menu. The IES Group Interface (Edit) form opens.

5 Configure the parameters:

- Auto-Assign ID
- Interface ID
- Name
- Description
- Administrative State
- MAC Address
- Trusted
- Operational State UP While Empty
- LNS
- Specific Type
- Enable WPP
- Enable Ingress Stats
- IPv6 Allowed
- IPv6 IPoE Bridged Mode Enabled
- QoS Route Lookup IPv4
- QoS Route Lookup IPv6
- Configured IP MTU



Note — The LNS parameter defines the type of group interface. This parameter is set at creation time and cannot be modified. Regular group interfaces cannot configure LNS attributes, and an LNS group interface does not allow PPPoE configuration or SAPs.

6 If you enabled the IPv6 Allowed parameter in step 5, configure IPv6 router advertisement and DHCPv6 on the group interface.

i Click on the IPv6 Advertisement tab and configure the parameters:

- Administrative State
- Current Hop Limit
- Managed Address Config
- Max Interval (seconds)
- Min Interval (seconds)
- Link MTU
- Other Stateful Config
- Reachable Time (milliseconds)
- Retransmit Time (milliseconds)
- Router Lifetime (seconds)
- Autonomous Address Configuration
- Preferred Life Time
- Valid Life Time

ii Click on the DHCPv6 tab.

iii Click on the Select button and select a local user database from the Select Local User Database form.

iv Click on the Proxy Server tab and configure the parameters:

- Administrative State
- Renew Timer
- Rebind Timer
- Valid Life Time
- Preferred Life Time
- Client Applications
- Server ID Type
- ID Type
- Value



Note — The ID Type and Value parameters are configurable only if the Server ID Type parameter is set to Enterprise.

v Click on the Relay tab and configure the parameters:

- Administrative State
- Description
- Remote ID
- Client Applications
- Link Address

vi Configure the Server 1 through Server 8 parameters.

vii Configure the interface name for each DHCPv6 server by clicking on the Select button in the Zone Index panel. The Select Zone Index - GrplfDhcpv6RelayCfg form opens with a list of local L3 access interfaces and network interfaces.

viii Choose an interface and click on the OK button. The Select Zone Index - GrplfDhcpv6RelayCfg form closes and the IES Group Interface form refreshes with the interface name.



Note — If you have entered a Unicast address, then the Interface Name parameter is not required.

7 If you enabled the Enable WPP parameter in step 5, configure WPP on the group interface.

i Click on the WPP tab.

ii Configure the Administrative State parameter.

iii Click on the Select button in the WPP Site panel and choose a WPP site from the Select WPP Site form.

iv Configure the Portal Name parameter.

v Click on the Select button beside the Initial Subscriber Profile parameter and choose a subscriber profile from the Select Subscriber Profile form.

vi Click on the Select button beside the Initial SLA Profile parameter and choose an SLA profile from the Select SLA Profile form.

vii Click on the Select button beside the Initial Application Profile parameter and choose an application profile from the Select Application Profile form.

viii Configure the Restore Default Profile On Disconnection parameter.

8 Click on the Anti-Spoofing tab.

9 Configure the ARP Populate parameter.

10 Click on the Subscriber Management tab.

11 Configure the parameters:

- SHCV Enabled
- SHCV Interval (minutes)
- SHCV Source
- SHCV Action
- SHCV Retry Timeout (seconds)
- SHCV Retry Count
- SHCV Family

12 Configure SRRP for the group interface, if required.

i Configure the parameters in the Routing panel:

- Enabled
- Hold Time (seconds)

ii Click on the SRRP tab.

iii Click on the Create button in the SRRP Instance panel. The SRRP Instance (Create) form opens with the General tab displayed.

iv Configure the parameters:

- SRRP ID
- Description
- Administrative State

v Click on the Select button in the Operational Group panel. The Select Monitored Group Name - SRRP Instance form opens.

vi Choose a Monitored Group Name and click on the OK button. The Select Monitored Group Name - SRRP Instance form closes.

vii Configure the Priority Step parameter.

viii Click on the Behavior tab.

ix Configure the General parameters:

- Gateway MAC Address
- Keep Alive Interval
- Priority
- Preempt
- FIB Population Mode
- One Gratuitous ARP Per SAP

x Click on the Select button in the Message Path panel. The Select Message Path Pointer - SRRP Instance form opens, displaying the SAPs available on the site.

xi Select the SAP you need to use for the in-band messaging between the sites and click on the OK button. The Select Message Path Pointer - SRRP Instance form closes.

xii Click on the Select button in the Policy Pointer 1 panel. The Select Policy Pointer 1 - SRRP Instance form opens.

xiii Choose an entry and click on the OK button. The Select Policy Pointer 1 - SRRP Instance form closes.

xiv Click on the Select button in the Policy Pointer 1 panel. The Select Policy Pointer 2 - SRRP Instance form opens.

xv Choose an entry and click on the OK button. The Select Policy Pointer 2 - SRRP Instance form closes.

xvi Click on the OK button. The SRRP Instance (Create) form closes and a dialog box appears.

xvii Click on the OK button.

13 Configure ICMP for the group interface, if required.

i Click on the ICMP tab.

ii Configure the parameters:

- Mask Reply
- Redirects
- Unreachables
- TTL Expired
- Number of Redirects
- Redirects Time (seconds)
- Number of Unreachables
- Unreachables Time (seconds)
- Number of TTL Expired
- TTL Expired Time (seconds)

14 Configure ARP for the group interface, if required.

i Click on the ARP tab. The General tab is displayed.

ii Configure the Timeout (seconds) parameter.

iii Click on the Proxy ARP tab.

iv Configure the parameters:

- Remote Proxy ARP
- Enable Local Proxy ARP
- Proxy ARP Policy 1 through Proxy ARP Policy 5

15 Configure DHCP relay for the group interface, if required.

i Click on the DHCP tab. The General tab is displayed.

ii Configure the parameters:

- Enable DHCP Relay
- Description
- Match Circuit ID
- Trusted
- Lease Populate
- L2 Header
- Anti-Spoof MAC Address

iii Depending on the type and release of device that you are configuring, the Subscriber Authentication Policy panel is present. Choose a Select Subscriber Authentication Policy, if required. Otherwise, go to step xiv.

iv Click on the Select button in the Subscriber Authentication Policy panel. The Select Subscriber Authentication Policy - GrpltfDhcpRelayCfg form opens.

v Configure the filter criteria, and click on the Search button. A list of available subscribers appears.

vi Choose a subscriber authentication policy and click on the OK button. The Select Subscriber Authentication Policy - GrpltfDchpRelayCfg form closes, and the IES Group Interface (Create) form refreshes with the subscriber authentication policy name.

vii Configure the parameters:

- Action
- Circuit ID
- Remote ID
- Remote ID String
- Vendor Specific Options
- Vendor String
- IP address (GI address)
- Use as source
- Relay Unicast Message



Note 1 — The Remote ID String parameter is configurable when the Remote ID is set to Remote IDString.

Note 2 — When the Relay Unicast Message parameter is set to Renew or Release Update Source IP, the GI address parameter can be configured as any local configured address in the same routing instance as the GI address for the DHCP relayed messages. If the Relay Unicast Message parameter is set to None, the GI address is restricted to the IP address configured on the subscriber interface.

viii Click on the Select button in the Local User Database panel to choose a local user database. The Select localUserDbPointer - GrpItfDhcpRelayCfg form opens.

ix Configure the filter criteria, and click on the Search button. A list of available databases appears.

x Choose a database and click on the OK button. The Select localUserDbPointer - GrpItfDhcpRelayCfg form closes, and the IES Group Interface (Create) form reappears with the database name information displayed.

xi Click on the Select button in the DHCP Filter panel to choose a filter policy to bind with the group interface. The Select dhcpFilterPointer - GrpItfDhcpRelayCfg form opens.

xii Configure the filter criteria, and click on the Search button. A list of available filter policies appears.

xiii Choose a filter policy and click on the OK button. The Select dhcpFilterPointer - GrpItfDhcpRelayCfg form closes, and the IES Group Interface (Create) form reappears with the filter policy information displayed.

xiv Click on the Server tab.

xv Configure the parameters:

- Server 1 to Server 8
- Administrative State
- Emulated Server IP Address
- Lease Time
- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time Override



Note — The following parameters are configurable when the Lease Time parameter is set to Specified Time Period.

- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time Override

16 Click on the Default Hosts tab to create a default host where the associated DHCP filter policy is configured with the Bypass Host creation action. See Procedure 44-7 for more information about DHCP filter creation. See step 15 xi for more information about how to bind a DHCP filter with the group interface.

i Click on the Create button. The Default Host (Create) form opens.

ii Click on the Select button in the Default Host Configuration panel to choose the Default Host IP Address parameter value for the DHCP filter policy to associate with the subscriber interface SAP. The Select Default Host Configuration form opens.

iii Configure the filter criteria, and click on the Search button. A list of available DHCP filter policies appears.

iv Choose a DHCP filter policy and click on the OK button. The Select Default Host Configuration form closes, and the Default Host (Create) form reappears with the IP address for the selected DHCP filter policy displayed.

v Configure the Next Hop IP Address parameter.

vi Click on the Apply button. The Default Host (Create) form closes and the default host is added to the Default Hosts list.

17 Click on the Client Applications tab. Configure the Client Applications parameter.

18 Configure PPP for the group interface, if required.

i Click on the PPP tab.

ii Configure the Description and Administrative State parameters in the PPPoE panel.

iii Click on the Select button beside the Policy field in the PPPoE panel and choose a PPPoE policy from the Select Policy form.

iv Click on the Select button beside the Local User DB field in the PPPoE panel and choose a PPPoE Local User DB from the The Select Local User DB form.

v Configure the remaining parameters in the PPPoE panel:

- Session Limit
- Session Limit per SAP
- Anti-Spoofing
- CCAG Use Original SAP
- Vendor Specific Option String

vi Configure the Description and Administrative State parameters in the PPP panel.

vii Click on the Select button beside the Policy field in the PPP panel and choose a PPP policy from the Select Policy form.

viii Click on the Select button beside the Local User DB field in the PPP panel and choose a PPP Local User DB from the The Select Local User DB form.

ix Configure the Session Limit parameter in the PPP panel

19 Configure the ARP host for the group interface, if required.

i Click on the ARP Host Configuration tab.

ii Configure the parameters:

- Administrative State
- ARP Host Limit
- Minimum Authentication Interval (minutes)
- SAP ARP Host Limit

20 Configure local address assignment for the group interface, if required.

i Click on the Local Address Assignment tab.

ii Configure the parameters:

- Administrative State
- Default Pool Name
- Secondary Pool Name

iii On the IPv4 Options panel, configure the PPP-v4 parameter and select a local DHCP server, if required.

iv On the IPv6 Options panel, configure the IPoE WAN and PPP SLAAC parameters and select a local DHCPv6 server, if required.

21 If you set the parameter LNS to TRUE in step 5, perform the following steps to configure LNS for the group interface.



Note — After you create an LNS group interface, you must configure the L2TP tunnel group profile or L2TP tunnel profile to terminate sessions for the LNS group interface; see Procedure 23-34 for more information. You can also configure the termination of sessions on a group interface using a RADIUS server.

i Click on the LNS tab.

ii Configure the Description parameter.

iii Click on the Select button in the Default Subscriber Profile panel. The Select Default Subscriber Profile (Terminate LNS PPP Sessions) form opens.

iv Choose a subscriber profile and click on the OK button. The Select Default Subscriber Profile (Terminate LNS PPP Sessions) form closes and the IES Group Interface (Create) form reappears with the Subscriber Profile displayed.

v Click on the Select button in the Default SLA Profile panel. The Select Default SLA Profile (Terminate LNS PPP Sessions) form opens.

vi Choose an SLA profile and click on the OK button. The Select Default SLA Profile (Terminate LNS PPP Sessions) form closes and the IES Group Interface (Create) form reappears with the SLA Profile displayed.

vii Click on the Select button in the Subscriber Identification Policy panel. The Select Subscriber Identification Policy (Terminate LNS PPP Sessions) form opens.

viii Choose a subscriber identification policy and click on the OK button. The Select Subscriber Identification Policy (Terminate LNS PPP Sessions) form closes and the IES Group Interface (Create) form reappears with the subscriber identification policy displayed.

ix Click on the Select button in the Default Application Profile panel. The Select Default Application Profile (Terminate LNS PPP Sessions) form opens.

x Choose a default application profile and click on the OK button. The Select Default Application Profile (Terminate LNS PPP Sessions) form closes and the IES Group Interface (Create) form reappears with the default application profile displayed.

22 Configure the Default Subscriber Identification Type parameter.

23 Click on the Service Access Points tab to configure SAPs for the group interface.

24 Click on the Create button. The IES Service Access Point (Create) form opens with the General tab displayed.

25 Configure the parameters:

- Name
- Description
- Administrative State
- Calling Station ID

26 Associate a host lockout policy with the group interface, if required. Click on the Select button in the Host Lockout panel to select a policy.

27 Click on the Port tab.

28 Click on the Select button to choose a port for the SAP. The Select Terminating Port - IES Service Access Point form opens.



Caution — The creation of a SAP that uses the same port and encapsulation values as an existing inactive MSAP fails under the following conditions:

- If you try to use the 5620 SAM to create a SAP, the configuration fails and the 5620 SAM displays an error message.
- If you use a CLI to create a SAP in a service other than the service that contains the MSAP, the configuration succeeds but the MSAP is inactive until the regular SAP is deleted. Although the 5620 SAM displays the SAP and MSAP, the MSAP remains inactive and consumes resources.
- If you use a CLI to create a SAP in the service that contains the MSAP, the SAP creation fails.

Alcatel-Lucent recommends that you delete an inactive MSAP from the 5620 SAM if you need to create a regular SAP on the same port using the same encapsulation values. See Procedure 65-34 for more information about deleting MSAPs.



Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

29 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - IES Service Access Point form closes, and the IES Service Access Point (Create) form displays the port information.

30 Configure the parameters:

- Outer Encapsulation Value
- Inner Encapsulation Value
- Outer Encapsulation Value (VPI)
- Inner Encapsulation Value (VCI)
- SAP Description
- SAP Administrative State

If the port uses dot1q encapsulation, you can enable the Auto-Assign ID parameter to have the Outer Encapsulation Value parameter automatically assigned. The system assigns the lowest unused encapsulation value.



Note — You can set the Auto-Assign ID parameter to be the default parameter for dot1q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter on the User Preferences form. Choose Application→ User Preferences from the main menu.

The Inner Encapsulation Value is configurable only when the port is an Ethernet or frame relay port with QinQ encapsulation.

The Outer Encapsulation Value (VPI) and Inner Encapsulation Value (VCI) parameters are configurable only for ATM ports.

31 Assign ingress and egress QoS policies to the SAP, if required.



Note — Items such as policies, schedulers, and filters can be applied later to multiple service components at once. Choose and right-click the components in the service navigation tree, choose Properties, and configure the parameters on the appropriate tab. This action opens a properties form in a new window for the component that was right-clicked. The navigation tree is not displayed in this new window.

i Click on the QoS tab.

ii Configure the parameters:

- Ingress Match QinQ Dot1P
- Egress Mark QinQ Top Bits Only
- Use SAP ID as Subscriber ID

iii Click on the Select button in the Ingress Policy panel. The Select Ingress Policy - IES Service Access Point form opens.

iv Configure the filter criteria and click on the Search button. A list of available ingress policies appear.

v Choose an ingress QoS policy and click on the OK button. The Select Ingress Policy - IES Service Access Point form closes, and the IES L3 Service Access Point (Create) form reappears with the ingress QoS policy information displayed.



Note — If you select an ingress policy which has a forwarding class mapped to an ingress queue group, you must ensure that the port you selected in step 29 has the access ingress queue group with the same name created on it.

See Procedure 16-1for more information about how to configure Ethernet ports. See chapter 42 for more information about queue group template policies.

vi Click on the Select button in the Egress Policy panel. The Select Egress Policy - IES L3 Service Access Interface form opens.

vii Configure the filter criteria and click on the Search button. A list of available egress policies is displayed.

viii Choose an egress QoS policy and click on the OK button. The Select Egress Policy - IES Service Access Point form closes, and the IES Service Access Point (Create) form reappears with the egress QoS policy information displayed.



Note — If you select an egress policy which has a forwarding class mapped to an egress queue group, you must ensure that the port you selected in step 29 has the access egress queue group with the same name created on it.

See Procedure 16-1 for more information about how to configure Ethernet ports. See chapter 42 for more information about queue group template policies.

32 Click on the Schedulers tab to configure scheduling; otherwise, go to step 34.



Note — The Schedulers tab is displayed only if a port is assigned to the SAP earlier in the procedure.

33 Perform one of the following.

a Specify that an aggregation scheduler policy is not applied to the SAP.

i Set the Aggregation parameter to off.



Note — The Aggregation parameter is not configurable if the port you selected in step 29 is an HSMDA port.

ii Configure the parameters:

- Aggregate Rate Limit (kbps)
- Frame-Based Accounting



Note 1 — The Aggregate Rate Limit (kbps) and Frame-Based Accounting parameters are displayed only when there is no scheduler specified in the Egress Scheduler panel.

Note 2 — The Frame-Based Accounting parameter is not configurable if the port you selected in step 29 is an HSMDA port.

Note 3 — You cannot specify an egress scheduler when the Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

iii Click on the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - IES Service Access Point form opens.

iv Choose an ingress scheduler and click on the OK button. The Select Ingress Scheduler - IES Service Access Point form closes, and the IES Service Access Point (Create) form refreshes with the ingress scheduler information displayed.

v Click on the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Ingress Policer Control Policy form opens.

vi Choose a policer control policy and click on the OK button. The Select Ingress Policer Control Policy form closes and the IES Service Access Point (Create) form reappears with the ingress policer control policy information displayed.

vii If the port you selected in step 29 is an HSMDA port, go to step 34.

viii Click on the Select button in the Select Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - IES Service Access Point form opens.

ix Choose an egress scheduler and click on the OK button. The Select Egress Scheduler - IES Service Access Point form closes, and the IES Service Access Point (Create) form refreshes with the egress scheduler information displayed.

x Click on the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Egress Policer Control Policy form opens.

xi Choose a policer control policy and click on the OK button. The Select Egress Policer Control Policy form closes and the IES Service Access Point (Create) form reappears with the egress policer control policy information displayed.

xii Go to step 34.

b Specify that an aggregation scheduler policy is applied to the SAP.



Note — You cannot specify an access scheduler policy if the port you selected in step 29 is an HSMDA port. Go to step 34.

i Set the Aggregation parameter to on.

ii Click on the Select button in the Aggregation Scheduler panel to choose an aggregation scheduler. The Select Aggregation Scheduler - IES Service Access Point form opens.

iii Choose an aggregation scheduler and click on the OK button. The Select Aggregation Scheduler - IES Service Access Point form closes, and the IES Service Access Point (Create) form refreshes with the aggregation scheduler information displayed.

34 Assign ingress and egress ACL filters to the SAP, if required.

i Click on the ACL tab.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter from the Select Ingress Filter - IES Service Access Point form.

iii Click on the Select button in the Egress Filter panel to choose an egress ACL filter from the Select Egress Filter - IES Service Access Point form.

35 Click on the Accounting tab to assign an accounting policy to the SAP.

i Click on the Select button to choose an accounting policy. The Select Accounting Policy - IES Service Access Point form opens.

ii Choose an accounting policy and click on the OK button. The Select Accounting Policy - IES Service Access Point form closes, and the IES Service Access Point (Create) form reappears with the accounting policy information displayed.

iii Configure the Collect Accounting Statistics parameter.

36 Click on the Anti-Spoofing tab to configure anti-spoofing for the SAP. The Anti-Spoofing tab opens with the General tab displayed.

i Configure the Anti-Spoofing parameter.

ii Click on the Static Hosts tab to configure a static subscriber host entry for each subscriber host that is not managed by DHCP.

iii Click on the Create button. The Access Interface Anti-Spoofing Static Host Display (Create) form opens.

iv Configure the parameters:

- IP Address
- MAC Address
- Subscriber Identification
- Use SAP ID as Subscriber ID
- ANCP String
- Intermediate Destination ID

v Click on the Select button in the Subscriber Profile panel to choose a subscriber profile for the static host, if required. The Select Subscriber Profile - AntiSpoofingStaticHosts form opens with the list of available subscriber profiles displayed.

vi Choose a subscriber profile and click on the OK button. The Select Subscriber Profile - AntiSpoofingStaticHosts form closes, and the subscriber profile name appears in the Subscriber Profile panel.

vii Click on the Select button in the SLA Profile panel to choose an SLA profile for the static host. The Select SLA Profile - AntiSpoofingStaticHosts form opens with the list of available SLA profiles displayed.

viii Choose an SLA profile and click on the OK button. The Select SLA Profile - AntiSpoofingStaticHosts form closes, and the SLA profile name appears in the SLA Profile panel.

ix Click on the Select button in the Application Profile panel to choose an application profile for the static host. The Select Application Profile - AntiSpoofingStaticHosts form opens with the list of application profiles on the NE displayed.

x Choose an application profile and click on the OK button. The Select Application Profile - AntiSpoofingStaticHosts form closes, and the application profile name appears in the Application Profile panel.

xi Click on the OK button. A dialog box appears.

xii Click on the OK button. The Access Interface Anti-Spoofing Static Host Display (Create) form closes.

37 Assign a DoS protection policy or DDoS protection policy to the SAP, if required.



Note — A default DoS protection policy is automatically assigned to the SAP.

i Click on the Security tab.

ii Click on the Select button in the NE DoS Protection panel and choose a DoS protection policy from the Select NE DoS Protection form.

iii Click on the Select button next to the NE DDoS Protection Policy field and choose a DDoS protection policy from the Select NE DDoS Protection Policy form.

iv Configure the parameters:

- MAC Monitoring
- IP Src Monitoring

38 Associate a MEP to the SAP, if required.

i Click on the MEPs tab.

ii Click on the Create button. The MEP (Create) form opens with the General tab displayed.

iii Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

iv Choose an entry and click on the OK button. The Select Maintenance Entity Group form closes.

v Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Propagation
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)
- CCM Padding Packet Size (Bytes)



Note — The CCM Padding Packet Size (Bytes) parameter cannot be configured when the CCM interval parameter is set to 10 ms or 100 ms.

39 If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab. Otherwise, go to step 43.

40 Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

41 Click on the AIS tab.

42 Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

43 Click on the OK button. The MEP (Create) form displays the SAP information.

44 Click on the OK button. The MEP (Create) form closes.

45 Click on the Subscriber Management tab to configure residential subscriber management on the SAP. The IGMP Host Tracking tab is displayed.

i Click on the Select button to choose the import policy used to filter IGMP packets. The Select SapIgmpHostTracking form opens.

ii Configure the filter parameters and click on the Search button. A list of import policies appears.

iii Choose a policy and click on the OK button. The selected import policy name appears.

iv Configure the parameters:

- Expiry Time (seconds)
- Maximum Number of Groups
- Maximum Number of Sources per Group
- Maximum Number of Group Sources per Group
- Disable Router Alert Check

v You can click on the Host Tracking Info tab to view a list of hosts that are being tracked on this service access point.

vi Click on the Profiles tab.

vii Configure the parameters:

- Admin Status
- Service Model
- Subscriber Limit
- Default Subscriber Identification Type
- Default Subscriber ID
- Default Intermediate Destination Id Type
- Default Intermediate Destination Id
- Profiled Traffic only
- Non-Subscriber Traffic Identification

viii Click on the Select button in the Default Subscriber Profile panel to choose a default subscriber profile for the SAP, if required. The Select Default Subscriber Profile form opens with the list of available subscriber profiles displayed.

ix Choose a subscriber profile and click on the OK button. The Select Default Subscriber Profile form closes, and the subscriber profile name appears in the Default Subscriber Profile panel.

x Click on the Select button in the Default SLA Profile panel to choose a Default SLA profile for the SAP, if required. The Select Default SLA Profile form opens with the list of available SLA profiles displayed.

xi Choose an SLA profile and click on the OK button. The Select Default SLA Profile form closes, and the SLA profile name appears in the Default SLA Profile panel.

xii Click on the Select button in the Subscriber Identification Policy panel to choose a subscriber identification policy for the SAP, if required. The Select Subscriber Identification Policy form opens with the list of available subscriber identification policies displayed.

xiii Choose a subscriber identification policy and click on the OK button. The Select Subscriber Identification Policy form closes, and the subscriber identification policy name appears in the Subscriber Identification Policy panel.

xiv Click on the Select button in the Default Application Profile panel to choose a default application profile for the SAP, if required. The Select Default Application Profile form opens with the list of application profiles on the NE displayed.

xv Choose an application profile and click on the OK button. The Select Default Application Profile form closes, and the application profile name appears in the Default Application Profile panel.

xvi Click on the Select button in the Non-Subscriber Traffic Subscriber Profile panel to choose a non-subscriber subscriber profile for the SAP, if required. The Select Non-Subscriber Traffic Subscriber Profile form opens with the list of available subscriber profiles displayed.

xvii Choose a subscriber profile and click on the OK button. The Select Non-Subscriber Traffic Subscriber Profile form closes, and the subscriber profile name appears in the Non-Subscriber Traffic Subscriber Profile panel.

xviii Click on the Select button in the Non-Subscriber Traffic SLA Profile panel to choose a Non-Subscriber Traffic SLA profile for the SAP, if required. The Select Non-Subscriber Traffic SLA Profile form opens with the list of available SLA profiles displayed.

xix Choose an SLA profile and click on the OK button. The Select Non-Subscriber Traffic SLA Profile form closes, and the SLA profile name appears in the Non-Subscriber Traffic SLA Profile panel.

xx Click on the Select button in the Non-Subscriber Traffic Application Profile panel to choose a non-subscriber traffic application profile for the SAP, if required. The Select Non-Subscriber Traffic Application Profile form opens with the list of application profiles on the NE displayed.

xxi Choose an application profile and click on the OK button. The Select Non-Subscriber Traffic Application Profile form closes, and the application profile name appears in the Non-Subscriber Traffic Application Profile panel.

46 Assign an ANCP policy to the SAP, if required.

i Click on the ANCP Static Map tab.

ii Click on the Create button. The ANCP Static Map (Create) form opens.

iii Configure the ANCP String parameter.

iv Click on the Select button to choose an ANCP Policy. The Select ANCP Policy - ANCP Static Map form opens.

v Choose an ANCP policy and click on the OK button. The Select ANCP Policy - ANCP Static Map form closes and the ANCP Static Map form reappears with the ANCP policy information displayed.

vi Click on the OK button. The ANCP Static Map form closes.

47 Configure ATM on the SAP, if required.

i Click on the ATM tab.

ii Configure the parameters:

- AAL5 Encapsulation
- ATM OAM Alarm Cell Handling
- Periodic ATM OAM Loopback

iii Click on the Select button in the Ingress ATM Policy panel to choose an ingress ATM policy. The Select Ingress ATM Policy - ATM Configuration form opens.

iv Choose an ingress ATM policy and click on the OK button. The Select Ingress ATM Policy - ATM Configuration form closes, and the IES Service Access Point (Create) form refreshes with the ingress ATM policy information displayed.

v Click on the Select button in the Egress ATM Policy panel to choose an egress ATM policy. The Select Egress ATM Policy - ATM Configuration form opens.

vi Choose an egress ATM policy and click on the OK button. The Select Egress ATM Policy - ATM Configuration form closes, and the IES Service Access Point (Create) form refreshes with the egress ATM policy information displayed.

48 Modify PPPoE Sessions that have been generated by the NE, for the group interface, if required. See chapter 65 for more information about viewing and configuring a PPPoE session.

49 Click on the OK button. The IES Service Access Point (Create) form closes, and a dialog box appears.

50 Click on the OK button. The IES Group Interface (Create) form refreshes to display the SAP.

51 To configure additional SAPs in the group interface, go to step 24.

52 Click on the OK button. The IES Group Interface (Create) form closes, and a dialog box appears.

53 Click on the OK button. The IES Service (Edit) form refreshes to display the SAP below the group interface.

54 Click on the OK button. A dialog box appears.

55 Click on the Yes button. The IES Service (Edit) form closes.

56 Close the Manage Services form.

Procedure 70-13 To configure a WLAN GW for an IES group interface

Before you can configure a WLAN GW for an IES group interface, you must configure an IES group interface with the Specific Type parameter set to Soft GRE. See Procedure 70-12.

1 Choose Manage→Service→Services from the navigation tree view selector. The Manage Services form opens.

2 Choose IES Site (IES) from the Object drop-down list.

3 Click on the Search button. A list of IES sites is displayed.

4 Select an IES site with an IES group interface and click on the Properties button. The IES Site form opens with the general tab displayed.

For the purposes of WLAN GW configuration, you must choose a Soft GRE type IES group interface.

5 On the IES Site form navigation tree, expand the Subscriber Interfaces icon.

6 Expand a subscriber interface with an IES group interface.

7 Click on an IES group interface. The general tab is displayed.

8 Click on the WLAN GW tab.

9 Click on the Select button in the WLAN GW Group panel and choose a WLAN GW group form the Select WLAN GW Group form.

10 Click on the Select button in the Tunnel Router Instance panel and choose a tunnel router instance from the Select Tunnel Router Instance form.

11 Configure the WLAN Gateway IPv4 Address and/or WLAN Gateway IPv6 Address parameter.

12 Click on the Select button in the Default Retail Service panel and choose a default retail IES service from the Select Default Retail Service form.

13 Configure the parameters:

- TCP Maximum Segment Size Adjustment
- Data Triggered UE Creation
- Mobility Detection Trigger
- Hold Time

14 Configure egress QoS, if required.

i In the Egress QoS panel, configure the parameters:

- Multi Client Only Shaping
- Shaping
- Hold Time
  Enabling the Infinite check box sets the Hold Time parameter to infinite.

ii Click on the Select button beside the QoS Policy field and choose an access egress policy from the Select QoS - Soft GRE Config form.

iii Click on the Select button beside the Scheduler Policy field and choose a scheduler policy from the Select Scheduler - Soft GRE Config form.

iv Configure the Aggregate Rate Limit parameter. Do not configure this parameter with a positive value if you specified a scheduler policy in step iii.

15 Click on the Select button beside the Authentication Policy field and choose an authentication policy from the Select ISA RADIUS Policies - Soft GRE Config form.

16 Configure an authentication hold time, if required:

i Enable the check box in the Authentication Hold Time panel.

ii Specify an authentication hold time in the Hours, Minutes, and Seconds fields.

17 Configure SAP parameters, as required.

i Click on the SAP Parameters tab.

ii Configure the Description parameter.

iii Click on the Select button beside the Subscriber Profile parameter and choose a subscriber profile from the Select Subscriber Profile form.

iv Click on the Select button beside the SLA Profile parameter and choose an SLA profile from the Select SLA Profile form.

v Click on the Select button beside the Application Profile parameter and choose an application profile from the Select Application Profile form.

vi Click on the Select button beside the Subscriber Identification Policy parameter and choose a subscriber identification policy from the Select Subscriber Identification Policy form.

vii Configure the Default ID Type parameter.

viii If the Default ID Type parameter was set to Use String, configure the Default ID String parameter.

18 Configure DHCP, as required.

i Click on the DHCP tab.

ii Configure the parameters:

- Administrative State
- L2 Aware IP Address
- IP Address Lease Time (Initial State)
  Remove the check mark from the Default check box and configure the Hours, Minutes, and Seconds parameters.
- IP Address Lease Time (Active State)
  Remove the check mark from the Default check box and configure the Hours, Minutes, and Seconds parameters.
- Primary DNS Server
- Secondary DNS Server
- Primary NBNS Server
- Secondary NBNS Server

iii Click on the Select button next to the NAT Policy field and choose a NAT policy from the Select NAT Policy form.

iv Click on the Select button next to the HTTP Redirect Policy field and choose an HTTP redirect policy from the Select HTTP Redirect Policy form.

19 Configure VLAN tag ranges, as required.

i Click on the VLAN Tag Ranges tab.

ii Click on the Create button. The VLAN Tag Range form opens.

iii Configure the parameters:

- Start VLAN Tag
- End VLAN Tag

iv Click on the Select button next to the Retail Service ID field and choose a retail service from the Select Retail Service form.

v Configure the Data Triggered User Equipment Creation parameter.

vi Click on the Select button next to the NAT Policy field and choose a NAT policy from the Select NAT Policy form.

vii Click on the Select button next to the HTTP Redirect Policy field and choose an HTTP redirect policy from the Select HTTP Redirect Policy form.

viii Click on the Select button next to the Authentication Policy field and choose an authentication policy from the Select Authentication Policy form.

ix Configure the Hold Time parameter. Remove the check mark from the Default check box and configure the Hours, Minutes, and Seconds parameters.

x Configure the Routing Instance parameter.

xi Click on the Select button in the RADIUS Proxy Cache panel and choose a RADIUS proxy cache server from the Select RADIUS Proxy Cache form.

xii Configure the MAC Address Format and Show Format parameters.

xiii Configure DHCP, as required.

xiv Click on the DHCP tab.

xv Configure the parameters:

- Administrative State
- L2 Aware IP Address
- IP Address Lease Time (Initial State)
  Remove the check mark from the Default check box and configure the Hours, Minutes, and Seconds parameters.
- IP Address Lease Time (Active State)
  Remove the check mark from the Default check box and configure the Hours, Minutes, and Seconds parameters.
- Primary DNS Server
- Secondary DNS Server
- Primary NBNS Server
- Secondary NBNS Server

xvi Click on the OK button. A dialog box appears.

xvii Click on the OK button. The VLAN Tag Ranges tab is updated with the new VLAN tag range displayed.

20 Click on the OK button. A dialog box appears.

21 Click on the OK button. The IES Site (Edit) form closes.

22 Close the Manage Services form.

Procedure 70-14 To add a TMS interface to an IES

The 7750 SR-7 and 7750 SR-12 devices support the configuration of a TMS interface in an IES.

The following conditions must be met before you can configure a TMS interface.

- You must have one IES configured.The TMS interface is configured on this on-ramp IES.
- You must have one VPRN configured for the off-ramp VPRN.
- Optionally, you can have one VPRN configured for the management VPRN.

- Each service must be associated within the same site on the same NE.
- The ISA-TMS daughter card must be installed.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears at the bottom of the Manage Services form.

3 Choose an IES and click on the Properties button. The IES Service Subscriber (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site to which you need to add the TMS interface; expand the entries for that site.

5 Right-click on the TMS Interfaces icon and choose Create TMS Interface. The TMS Interface (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- IPv6 Allowed



Note — The Name value for a TMS interface must be unique in the context of the IES Site. That is, there cannot be another L3 access interface, subscriber interface, group interface or TMS interface with the same name on the same IES site.

7 Assign an off-ramp VPRN to the TMS interface

i Click on the Select button in the Off-Ramp VPRN panel and select a VPRN from the Select Off-Ramp VPRN - TMS Interface form.

ii Click on the OK button. The Select Off-Ramp VPRN - TMS Interface form closes, and the TMS Interface (Create) form reappears with the VPRN information displayed.

8 Assign a management VPRN to the TMS interface

i Click on the Select button in the Management VPRN panel and select a VPRN from the Select Management VPRN - TMS Interface form.

ii Click on the OK button. The Select Management VPRN - TMS Interface form closes, and the TMS Interface (Create) form reappears with the subscriber information displayed.

9 Associate an ISA-TMS daughter card with the TMS interface.



Note — An ISA-TMS card can only be assigned to one TMS interface.

i Click on the Select button in the TMS Info panel and select an ISA-TMS to associate with the TMS interface from the Select ISA-TMS - TMS Interface form.

ii Click on the OK button. The Select ISA-TMS - TMS Interface form closes, and the TMS Interface (Create) form reappears with the slot name for the daughter card displayed.

10 Configure the ISA-TMS Authentication parameter.

11 Assign an IP address to the TMS interface.

i Click on the Addresses tab.

ii Click on the Create button. The IP Address (Create) form opens.

iii Configure the parameters:

- Address ID
- IP Address
- Prefix Length

iv Click on the OK button. The IP Address (Create) form closes, and a dialog box appears.

v Click on the OK button. The TMS Interface (Create) form reappears with the assigned IP addresses displayed.

12 Click on the OK button. The TMS Interface (Create) form closes, and a dialog box appears.

13 Click on the OK button. The IES Service Subscriber (Edit) form reappears with the new TMS interface displayed in the service navigation tree.

14 Click on the OK button. A dialog box appears.

15 Click on the Yes button. The IES Service Subscriber (Edit) form closes, and the Manage Services form reappears.

16 Close the Manage Services form.

Procedure 70-15 To implement dual homing using SRRP

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose an IES service and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Specify the pair of sites that are to participate in dual homing.



Note — The sites can be from different services.

5 Ensure that the pair of sites each contains a properly configured subscriber interface and SAPs underneath the group interface that will be participating in the redundant configuration.

6 Ensure that all subscriber interface IP addresses have a gateway address configured on them.

7 Create the Redundant Interface (used for SRRP out-of-band messaging) between the two routers.

i On the navigation tree, click on the site; expand the entries for that site.

ii Right-click on the Redundant Interfaces item for one site of the redundant pair, and choose Create Redundant Interface. The Redundant Interface (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State

iv Click on the Addresses tab.

v Click on the Create button. The IP Address (Create) form opens.

vi Specify IP addresses for the redundant interface on the current and remote sites. Configure the parameters:

- Address ID
- IP Address (in the form d.d.d.d, where d is a value from 0 to 255)
- Prefix Length
- Remote IP Address
- Broadcast Address Format



Note — The remote IP address must be on the same subnet as the current site's redundant interface IP Address. For example, if the current site's IP Address is 7.7.7.7, with a Prefix Length of 24, then the remote site's redundant interface address must be 7.7.7.d, where d is a value from 0 to 255, excluding 7.

vii Click on the OK button. The IP Address (Create) form closes, and a dialog box appears.

viii Click on the OK button. The Redundant Interface (Create) form reappears with the assigned redundant interface IP addresses displayed.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Redundant Interface (Create) form for the current site closes.

8 Create an SDP spoke binding between the current and remote sites. The Source Interface is the Redundant Interface you created in step 7 and the Tunnel Termination SIte is the remote site. The Return Tunnel must come from the remote site.

9 Assign the Redundant Interface to the Group Interface for the current site.

i On the navigation tree under Subscriber Interfaces, right-click on the group interface you need to use and choose Properties. The IES Group Interface (Edit) form opens with the General tab displayed.

ii Click on the Select button in the Redundant Interface panel. The Select Redundant Interface - IES Group Interface form opens.

iii Configure the list filter parameters if required and click on the Search button. A list of redundant interfaces on the site appears at the bottom of the form.

iv Select the Redundant Interface you created in step 7 and click on the OK button. The Select Redundant Interface - IES Group Interface form closes and the interface you selected appears in the Redundant Interface field.

v Click on the OK button. The IES Group Interface (Edit) form closes.

10 Create an SRRP Instance for the current site.

i On the navigation tree under group interfaces, right-click on the SRRP Instances item for the current site, and choose Create SRRP Instance. The SRRP Instance (Create) form opens with the General tab displayed.

ii Configure the parameters:

- SRRP ID
- Description
- Administrative State

The SRRP ID must be the same value for both the current and remote sites.

iii Click on the Behavior tab.

iv Configure the parameters:

- Gateway MAC Address
- Keep Alive Interval
- Priority
- FIB Population Mode

v Configure the message path by clicking the Select button in the Message Path panel. The Select Message Path Pointer - SRRP Instance form opens, displaying the SAPs available on the site.

vi Select the SAP you need to use for the in-band messaging between the sites.

vii Click on the OK button. The Select Message Path Pointer - SRRP Instance form closes.

viii Configure policy pointer 1, if required, by clicking the Select button in the Policy Pointer 1 panel. The Select Policy Pointer 1 - SRRP Instance form opens, displaying the pointers available on the site.

ix Select the pointer you need to use.

x Click on the OK button. The Select Policy Pointer 1 - SRRP Instance form closes.

xi Configure policy pointer 2, if required, by clicking the Select button in the Policy Pointer 2 panel. The Select Policy Pointer 2 - SRRP Instance form opens, displaying the pointers available on the site.

xii Select the pointer you need to use.

xiii Click on the OK button. The Select Policy Pointer 2 - SRRP Instance form closes.

xiv Click on the OK button. The SRRP Instance (Create) form closes, and a dialog box appears.

xv Click on the OK button. The IES Service (Edit) form reappears with the SRRP Instance displayed.

11 Click on the Turn Up button to activate the SRRP instance.

12 Repeat steps 7 to 11 for the remote site.



Note 1 — When you repeat steps 7 to 11 for the remote site, that site becomes the current site and the previously configured site is the remote site.

Note 2 — After the two sites have been properly set up, you can examine the SRRP peer associations at any time by right-clicking an SRRP Instance in the service's navigation tree. This opens the SRRP Instance - Edit form, which contains a read-only field called SRRP Peer. The Site ID, Service ID, and Operational State of the associated peer appear in this field.

You can also examine the state of an SRRP Instance by checking the Operational Flags field. The flags indicate specific problems that might occur with the SRRP Instance, as follows:

- Duplicate Subscriber IF Address: one of the local subscriber IP addresses is the same as a subscriber IP address on the remote NE.
- Redundant Interface Mismatch: the local SRRP instance and remote SRRP instance have mismatched redundant interfaces.
- SAP Mismatch: the local SRRP instance is backing a different set of SAPs than the peer.
- Subnet Mismatch: one of the subnets that SRRP is backing up does not have a match with the peer.
- Dual Master: both SRRP instances are master at the same time.
- SAP Tag Mismatch: the local SRRP instance is backing a set of SAPs with different remote and local tags.
- SRRP ID Mismatch: the peer has a different SRRP instance ID backing the same subnet.

13 Click on the OK button. A dialog box appears.

14 Click on the OK button. The IES Service (Edit) form closes.

Procedure 70-16 To configure IGMP host tracking on an IES site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES service and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Right-click on a Site icon and choose Properties from the contextual menu. The IES Site (Edit) form opens with the General tab displayed.

6 Click on the Multicast tab.

7 Click on the IGMP Host Tracking tab.

8 Configure the parameters:

- Expiry Time (seconds)
- Administrative State

9 Click on the OK button to close the IES Site (Edit) form.

10 Close the IES Service (Edit) form.

11 Close the Manage Services form.

Procedure 70-17 To configure an L3 access interface on an IES site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 On the navigation tree, click on the site to which you need to add the access interface; expand the entries for that site.

5 Right-click on L3 Access Interfaces and choose Create IES L3 Access Interface. The IES L3 Access Interface (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- MAC Address
- Allow Directed Broadcasts
- Loopback Enabled
- Cflowd Type
- Class
- Trusted
- IPv6 Allowed
- Admin Link Local Address
- Admin Link Local Address Preferred
- Enable Ingress FlowSpec IPv4
- Enable Ingress FlowSpec IPv6
- QoS Route Lookup IPv4
- QoS Route Lookup IPv6
- Calling Station ID
- Enable Ingress Stats
- Enable MAC Accounting Stats
- Configured IP MTU (Octets)
- Unnumbered Type
- IP Address
- Interface Name
- URPF Check State IPv4
- URPF Check Mode IPv4
- URPF Check State IPv6
- URPF Check Mode IPv6
- Tunnel Fault Notification
- PTP HW Assist

The Unnumbered Type parameter is configurable when the Class parameter is set to Unnumbered.

The Unnumbered Type parameter is configurable when the Class parameter is set to Unnumbered.

The IP Address parameter is configurable when the Unnumbered Type parameter is set to IP Address.

The Interface Name parameter is configurable when the Unnumbered Type parameter is set to Name.

The Admin Link Local Address and Admin Link Local Address Preferred parameters are only configurable when the IPv6 Allowed parameter is enabled.

The Enable Ingress FlowSpec IPv4 and Enable Ingress FlowSpec IPv6 parameters appear only when a port is configured on the interface.

The URPF Check State IPv6 and URPF Check Mode IPv6 parameters are only configurable when the IPv6 Allowed parameter is enabled.

The Tunnel Fault Notification parameter is configurable on interfaces where the device has ports configured in access or hybrid mode with QinQ encapsulation.

If you are configuring a tunnel facility MEP, Tunnel Fault Notification must be set to Accept, in order to receive the fault notification from the tunnel facility MEP.

7 If the Loopback Enabled parameter in step 6 is enabled, you cannot associate a port with the L3 interface. Go to step 16.

8 Bind an application profile to the IES L3 access interface, if required:

i Click on the Select button beside the Application Profile parameter in the Application Assurance panel. The Application Profile String: - IES L3 Access Interface list form opens.

ii Choose a profile and click on the OK button. The Application Profile String - IES L3 Access Interface list form closes and the L3 Access Interface (Create) form is refreshed with the Application Profile information.



Note — The Application Profile String: - IES L3 Access Interface list form only displays local profiles that already exist on the NE.

9 Choose one of the following AA transit policy types, if required.



Note 1 — You can only associate one AA transit policy type with a service object.

Note 2 — To bind a transit policy to an L3 access interface, a port must already exist on the interface.

Note 3 — You can bind a transit policy to only one L3 access interface or spoke SDP binding per NE.

Note 4 — The transit policy and the application profile must belong to the same application assurance group or partition.

a Associate an AA transit IP policy with the service object:

i Click on the Select button in the Transit IP Policy panel. The Select Transit IP Policy form opens.

ii Choose a transit IP policy and click on the OK button.

b Associate an AA transit prefix policy with the service object:

i Click on the Select button in the Transit Prefix Policy panel. The Select Transit Prefix Policy form opens.

ii Choose a transit IP policy and click on the OK button.

10 Associate a host lockout policy with the L3 access interface, if required. Click on the Select button in the Host Lockout panel to select a policy.

11 Click on the Port tab.

12 Click on the Select button to choose a port for the L3 access interface. The Select Terminating Port - IES L3 Access Interface form opens.



Note 1 — The form lists only ports in access or hybrid mode, or PW ports. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. The port is then listed when you click on the Search button.

Note 2 — The form only lists PW ports that are bound to a service tunnel. See Procedure 27-1 for information about creating a service tunnel with a PW port binding.

13 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - IES L3 Access Interface form closes, and the IES L3 Access Interface (Create) form displays the port information.

Once the port is selected, a number of other tabs are also displayed on the form.

14 Configure the parameters:

- Outer Encapsulation Value
- Inner Encapsulation Value
- Outer Encapsulation Value (VPI)
- Inner Encapsulation Value (VCI)
- SAP Description
- SAP Administrative State

If the port uses dot1q encapsulation, you can enable the Auto-Assign ID parameter to have the Outer Encapsulation Value parameter automatically assigned. The system assigns the lowest unused encapsulation value.



Note — You can set the Auto-Assign ID parameter to be the default parameter for dot1q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter on the User Preferences form. Choose Application→ User Preferences from the main menu.

The Inner Encapsulation Value is configurable only when the port is an Ethernet or frame relay port with QinQ encapsulation.

The Outer Encapsulation Value (VPI) and Inner Encapsulation Value (VCI) parameters are configurable only for ATM ports.

15 If the selected port uses FR encapsulation, configure frame relay for the interface.

i Click on the Frame Relay tab.

ii Set the FRF-12 Mode parameter to Enabled.

iii Configure the parameters:

- FRF-12 End-To-End Fragment Threshold
- Scheduling Class
- Fragment Interleave



Note — If a bundle was selected in step 13, only the Scheduling Class parameter are configurable.

16 Click on the OK button. The IES L3 Access Interface (Create) form closes, and the IES Service (Edit) form reappears with the new interface information displayed in the service navigation tree.

17 Close the IES Service (Edit) form.

18 Close the Manage Services form.

Procedure 70-18 To configure custom object attributes for AA reporting to the 5670 RAM on an IES L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The IES L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the 5670 RAM Parameters tab.

8 Click on the Reporting tab.

9 Click on the Create button. The AA Reporting (Create) form opens.

10 Configure the parameters:

- Customer Name
- Subscriber Name
- Subscriber Class
- Subscriber Type
- Total Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 1 Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 2 Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 3 Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 4 Bandwidth Upstream (Kbps)
- Downstream (Kbps)

11 Click on the OK button. The AA Reporting (Create) form closes and the reporting object is displayed in the list.

12 Close the IES L3 Access Interface (Edit) form.

13 Close the IES Service (Edit) form.

14 Close the Manage Services form.

Procedure 70-19 To bind an IES L3 access interface to a VPLS site or VPLS I-site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The IES L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Routed VPLS tab.



Note 1 — The operational state of the IP interface binding will not be turned up until the Enable IP Interface Binding parameter is set to true.

Note 2 — You can create and manage a routed VPLS connector from the navigation tree on the Composite Service (Edit) form.

8 Enter a VPLS site name or click on the Select button beside the VPLS Name parameter to choose a VPLS site with a configured site name. The Routed VPLS String - IES L3 Access Interface form opens.

9 Choose a VPLS site and click on the OK button. The VPLS site is displayed.

10 In the Ingress - IPv4 Filter panel, click on the Select button. The Select IPv4 Filter - IES L3 Access Interface form opens.

11 Choose an IPv4 filter and click on the OK button. The IPv4 filter information is displayed.

12 In the Ingress - IPv6 Filter panel, click on the Select button. The Select IPv6 Filter - IES L3 Access Interface form opens.

13 Choose an IPv6 filter and click on the OK button. The IPv6 filter information is displayed.

14 In the Egress - QoS Policy panel, click on the Select button. The Select QoS Policy - IES L3 Access Interface form opens.

15 Choose a QoS Policy and click on the OK button. The QoS Policy information is displayed.

16 Close the IES L3 Access Interface (Edit) form.

17 Close the IES Service (Edit) form.

18 Close the Manage Services form.

Procedure 70-20 To apply OSPF, RIP, or IS-IS to an IES L3 interface



Note — OSPF, RIP, or IS-IS must be enabled at the routing instance level before you can apply OSPF, RIP, or IS-IS to an L3 interface.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria.A list of services appears at the bottom of the Manage Services form.

3 Choose an IES and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Click on the Interfaces tab. The TMS Interfaces tab is displayed.

5 Click on the L3 Access Interfaces tab.

6 Choose an L3 interface in the list and click on the Properties button. The L3 Access Interface (Edit) form opens.

7 Click on the Protocols tab.

8 Click on the Create button. The Create Interface form opens.

9 Specify the interface type by configuring the What type of interface would you like to create? parameter.

10 Click on the OK button. The Interface (Create) form opens. See section 23.2 for information about configuring specific routing protocols.

Procedure 70-21 To assign ingress and egress QoS policies to an IES L3 access interface

Perform this procedure to assign ingress and egress QoS policies to an IES L3 access interface on a 7950 XRS, 7750 SR, 7450 ESS, 7710 SR, or 7705 SAR. See Procedure 70-22 for information on configuring QoS policies for the 7210 SAS.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The IES L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the QoS tab.



Note — The QoS tab is configurable only if a port is assigned to the interface.

8 Configure the Ingress Match QinQ Dot1P parameter.

9 Click on the Select button in the Ingress Policy panel to choose an ingress QoS policy. The Select Ingress Policy - IES L3 Access Interface form opens.

10 Choose an ingress QoS policy and click on the OK button. The Select Ingress Policy - IES L3 Access Interface form closes. The IES L3 Access Interface (Create) form refreshes with the ingress QoS policy information displayed.



Note — If you select an ingress policy which has a forwarding class mapped to an ingress queue group, you must ensure that the port configured on the interface uses the same access ingress queue group.

See Procedure 16-1 in chapter 16 for information about configuring Ethernet ports. See chapter 42 for information about queue group template policies.

11 Click on the Ingress Queue Group Template Policy Select button in the Forwarding Plane Redirect panel to choose a policy. The Select Forwarding Plane Queue Group Instance form opens.

12 Choose a policy and click on the OK button. The Select Forwarding Plane Queue Group Instance form closes. The IES L3 Access Interface (Create) form refreshes with the Ingress Queue Group Template Policy information displayed.

13 Configure the Instance ID parameter.

14 Configure the Egress Mark QinQ Top Bits Only parameter.

15 Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - IES L3 Access Interface form opens.

16 Choose an egress QoS policy and click on the OK button. The Select Egress Policy - IES L3 Access Interface form closes. The IES L3 Access Interface (Create) form refreshes with the egress QoS policy information displayed.



Note — If you select an egress policy that has a forwarding class mapped to an egress queue group, you must ensure that the port configured on the interface uses the same access egress queue group.

See Procedure 16-1 in chapter 16 for information about configuring Ethernet ports. See chapter 42 for information about queue group template policies.

17 Click on the Select button in the Port Redirect panel to choose an Egress Queue Group Template Policy, if required. The Select Egress Queue Group Template Policy form opens.



Note — Selecting an Egress Queue Group Template Policy here permits the redirection of Ethernet traffic packets to a queue ID specified in the SAP's egress port queue group. The following properties and restrictions apply:

- If an Egress Queue Group Template Policy is specified here, the policy must have port redirection enabled.
- You cannot use policy-based redirection with the queue group when the SAP has SAP-based redirection enabled.
- Port access egress redirection is only supported on Ethernet/LAG ports. It is not supported on SAPs bound on non-Ethernet, Eth-tunnel, or CCAG ports.
- Supported ports include access, hybrid, and HSMDA.
- Queue groups can be applied to SAPs that incorporate LAGs. The LAGs can include port members from just a single card or from multiple cards.
- If you edit a LAG incorporated by the SAP, you cannot remove the last LAG member if a queue group reference exists to the containing SAP.
- You cannot add a secondary LAG member that has a queue group mismatch with primary LAG member.

18 Choose an Egress Queue Group Template Policy and click on the OK button. The Select Egress Queue Group Template Policy form closes, and the IES L3 Access Interface (Create) form refreshes with the Egress Queue Group Template Policy information displayed.

19 If you are configuring an L3 access interface for a 7710 SR or 7705 SAR, or if the port that is configured on the interface is not an HSMDA port, then go to step 26.

20 Configure the Packet Byte Offset (bytes) parameter, if required. You must enable the associated Override check box if you need to configure this parameter.

21 Click on the Select button in the Egress HSMDA Override panel to choose a WRR policy. The Select WRR Policy form opens.

22 Choose a WRR policy and click on the OK button. The Select WRR Policy form closes and the IES L3 Access Interface (Create) form reappears with the WRR policy information displayed.

23 Click on the Select button in the Egress HSMDA Override panel to choose an HSMDA egress secondary shaper policy. The Select Secondary Shaper form opens.

24 Choose a secondary shaper and click on the OK button. The Select Secondary Shaper form closes and the IES L2 Access Interface (Create) form reappears with the secondary shaper information displayed.

25 Configure the parameters:

- Use Shared Queue
- Use Multipoint Shared Queue

26 Close the IES L3 Access Interface (Edit) form.

27 Close the IES Service (Edit) form.

28 Close the Manage Services form.

Procedure 70-22 To assign ingress and egress QoS policies to an IES L3 access interface on the 7210 SAS

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The IES L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Select button in the 7210 Specific panel to choose a SAS ingress policy. The Select SAS Ingress Policy - L2 Access Interface form opens.

8 Choose a SAS ingress policy and click on the OK button. The Select SAS Ingress Policy - L2 Access Interface form closes and the information is displayed.



Note — To support H-metering, you must choose a SAS ingress policy with all meter rate modes set to trtcm2.

9 Configure the following parameters in the Aggregate Rate Limit panel:

- Ingress Meter
- Ingress Meter Rate (kbps)
- Ingress Meter Burst



Note 1 — You can configure the Ingress Meter parameter only during SAP creation on the 7210 SAS-M and 7210 SAS-X. The parameter must be set to true to support H-metering.

Note 2 — You can configure the Ingress Meter Rate (kbps) and Ingress Meter Burst parameters only after SAP creation on the 7210 SAS-M and 7210 SAS-X.

10 Close the IES L3 Access Interface (Edit) form.

11 Close the IES Service (Edit) form.

12 Close the Manage Services form.

Procedure 70-23 To configure scheduling on an IES L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES service and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The IES L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Schedulers tab.

Note — The Schedulers tab is configurable only if a port is assigned to the SAP.

8 To configure scheduling on a 7705 SAR site, perform the following steps. Otherwise, go to step 9.

Note 1 — For the 7705 SAR, scheduler behavior is determined by the scheduler mode, which is 4-Priority by default. You can only configure the Egress and Ingress Aggregate Rate Limit parameters when the Scheduler Mode parameter is set to 16-Priority. You can set the Scheduler Mode to 16-Priority only when the port is on an MDA that supports 16-Priority. See the 7705 SAR documentation for more information.

Note 2 — If you change the Scheduler Mode parameter from 16-Priority to 4-Priority, the 5620 SAM automatically restores the default settings for the Egress Aggregate Rate Limit and Ingress Aggregate Rate Limit panels when you click on the Apply or OK button.

i In the Egress Scheduler panel, configure the Scheduler Mode parameter.

ii In the Ingress Scheduler panel, configure the Scheduler Mode parameter.

iii If you set the Scheduler Mode parameter to 16-Priority in the Egress Scheduler panel or Ingress Scheduler panel, configure the parameters in the Egress Aggregate Rate Limit panel and Ingress Aggregate Rate Limit panel, as required. Otherwise, go to step 11.

- Assign Aggregate Rate Limit
- Aggregate Rate Limit (kbps)
- Assign Aggregate CIR
- Aggregate CIR (kbps)

iv Go to step 11.

9 Specify that an aggregation scheduler policy is not applied to the interface. Otherwise, go to step 10.

i Set the Aggregation parameter to Off.



Note — The Aggregation parameter is not configurable if the port assigned to the SAP is an HSMDA port.

ii Configure the parameters:

- Aggregate Rate Limit (kbps)
- Frame-Based Accounting



Note 1 — The Aggregate Rate Limit (kbps) and Frame-Based Accounting parameters are configurable only when there is no scheduler specified in the Egress Scheduler panel.

Note 2 — The Frame-Based Accounting parameter is not configurable if the port assigned to the SAP is an HSMDA port.

Note 3 — You cannot specify an egress scheduler when the Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

iii Click on the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - IES L3 Access Interface form opens.

iv Choose an ingress scheduler and click on the OK button. The Select Ingress Scheduler - L3 Access Interface form closes, and the IES L3 Access Interface (Create) form refreshes with the ingress scheduler information displayed.

v Click on the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Policer Control Policy form opens.

vi Choose a policer control policy and click on the OK button. The Select Policer Control Policy form closes and the IES L3 Access Interface (Edit) form reappears with the ingress policer control policy information displayed.

vii If the port assigned to the SAP is an HSMDA port, go to step 11.

viii Click on the Select button in the Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - IES L3 Access Interface form opens.

ix Choose an egress scheduler and click on the OK button. The Select Egress Scheduler - IES L3 Access Interface form closes, and the L3 Access Interface (Create) form refreshes with the egress scheduler information displayed.

x Click on the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Policer Control Policy form opens.

xi Choose a policer control policy and click on the OK button. The Select Policer Control Policy form closes and the IES L3 Access Interface (Edit) form reappears with the egress policer control policy information displayed.

xii Go to step 11.

10 Specify that an aggregation scheduler policy is applied to the interface.



Note — You cannot specify an access scheduler policy if the port assigned to the SAP is an HSMDA port. Go to step 11.

i Set the Aggregation parameter to on.

ii Click on the Select button in the Aggregation Scheduler panel to choose an aggregation scheduler. The Select Aggregation Scheduler - IES L3 Access Interface form opens.

iii Choose an aggregation scheduler and click on the OK button. The Select Aggregation Scheduler - IES L3 Access Interface form closes, and the IES L3 Access Interface (Edit) form refreshes with the aggregation scheduler information displayed.

11 Close the IES L3 Access Interface (Edit) form.

12 Close the IES Service (Edit) form.

13 Close the Manage Services form.

Procedure 70-24 To assign ingress and egress ACL filters to an IES L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The IES L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the ACL tab.

8 Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - IES L3 Access Interface form opens.

9 Choose an ingress ACL filter and click on the OK button. The Select Ingress Filter - IES L3 Access Interface form closes, and the IES L3 Access Interface (Create) form reappears with the ingress ACL filter information displayed.

10 Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - IES L3 Access Interface form opens.

11 Choose an egress ACL filter and click on the OK button. The Select Egress Filter - IES L3 Access Interface form closes, and the IES L3 Access Interface (Create) form reappears with the egress ACL filter information displayed.

12 Click on the Select button in the IPv6 Ingress Filter panel to choose an ingress IPv6 ACL filter. The Select IPv6 Ingress Filter - IES L3 Access Interface form opens.

13 Choose an ingress IPv6 ACL filter and click on the OK button. The Select IPv6 Ingress Filter - IES L3 Access Interface form closes, and the IES L3 Access Interface (Create) form reappears with the ingress IPv6 ACL filter information displayed.

14 Click on the Select button in the IPv6 Egress Filter panel to choose an IPv6 egress ACL filter. The Select IPv6 Egress Filter - IES L3 Access Interface form opens.

15 Choose an IPv6 egress ACL filter and click on the OK button. The Select IPv6 Egress Filter - IES L3 Access Interface form closes, and the IES L3 Access Interface (Create) form reappears with the IPv6 egress ACL filter information displayed.

16 Close the IES L3 Access Interface (Edit) form.

17 Close the IES Service (Edit) form.

18 Close the Manage Services form.

Procedure 70-25 To associate a local DHCPv4 or DHCPv6 server to an IES L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES service and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The IES L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Local DHCP tab and perform one of the following steps.



Note — To associate local DHCPv6 servers, the IPv6 Allowed parameter must be enabled.

a For local DHCPv4 servers, click on the Select button in the Local DHCP Server panel and choose a local DHCP server from the Select Local DHCP Server - IES L3 Access Interface form.

b For local DHCPv6 servers, click on the Select button in the Local DHCPv6 Server panel and choose a local DHCPv6 server from the Select Local DHCPv6 Server - IES L3 Access Interface form.



Note — You cannot associate a local DHCPv4 server to the L3 group Interface if the Administrative State parameter in the Local Proxy Service panel is up.

8 Close the IES L3 Access Interface (Edit) form.

9 Close the IES Service (Edit) form.

10 Close the Manage Services form.

Procedure 70-26 To assign an accounting policy to an IES L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES service and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The IES L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Accounting tab.

8 Configure the Collect Accounting Statistics parameter.

9 Click on the Select button to choose an accounting policy. The Select Accounting Policy - IES L3 Access Interface form opens.

10 Choose an accounting policy and click on the OK button. The Select Accounting Policy - IES L3 Access Interface form closes and the IES L3 Access Interface (Edit) form reappears with the accounting policy information displayed.

11 Close the IES L3 Access Interface (Edit) form.

12 Close the IES Service (Edit) form.

13 Close the Manage Services form.

Procedure 70-27 To assign an ANCP policy to an IES L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES service and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The IES L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the ANCP Static Map tab.

8 Click on the Create button. The ANCP Static Map (Create) form opens with the General tab displayed.

9 Configure the ANCP String parameter.

10 Click on the Select button in the ANCP Policy panel to choose an ANCP policy. The Select ANCP Policy - ANCP Static Map list form opens.

11 Choose an ANCP policy and click on the OK button. The Select ANCP Policy - ANCP Static Map form closes and the ANCP Static Map form reappears with the ANCP policy information displayed.

12 Click on the OK button. A dialog box appears.

13 Click on the OK button. The ANCP Static Map (Create) form closes.

14 Close the IES L3 Access Interface (Edit) form.

15 Close the IES Site (Edit) form.

16 Close the IES Service (Edit) form.

17 Close the Manage Services form.

Procedure 70-28 To assign a time of day suite to an IES L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES service and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The IES L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the TOD Suite tab.

8 Click on the Select button beside the Name parameter. The Select Time Of Day Suite - IES L3 Access Interface list form opens.

9 Choose a time of day suite and click on the OK button. The Select Time Of Day Suite - IES L3 Access Interface list form closes, and the IES L3 Access Interface (Create) form refreshes with the time of day suite name.

Note 1 — You cannot assign a ToD suite to a L3 access interface if accounting statistics collection is enabled on the interface. You must first disable the Collect Accounting Statistics parameter in step 8 of Procedure 70-26.

Note 2 — SapEgrQosPlcyStats and SapIngQosPlcyStats statistics are collected only if a Time Of Day Suite is applied on the SAP.

10 Close the IES L3 Access Interface (Edit) form.

11 Close the IES Service (Edit) form.

12 Close the Manage Services form.

Procedure 70-29 To configure residential subscriber management for an IES L3 access interface

Residential subscriber management is supported on the 7450 ESS in mixed mode, 7750 SR, and 7710 SR.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES service and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The IES L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Subscriber Management tab. The Host Connectivity tab is displayed.

8 Select the SHCV Enabled parameter to enable SHCV.

9 Configure the parameters:

- SHCV Interval (minutes)
- SHCV Source
- SHCV Action
- SHCV Retry Timeout (seconds)
- SHCV Retry Count

10 Close the IES L3 Access Interface (Edit) form.

11 Close the IES Service (Edit) form.

12 Close the Manage Services form.

Procedure 70-30 To assign a DoS protection policy or DDoS protection policy to an IES L3 access interface



Note — A default DoS protection policy is automatically assigned to the interface.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The IES L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Security tab.

8 Click on the Select button in the NE DoS Protection panel and choose a DoS protection policy from the Select NE DoS Protection form.

9 Click on the Select button next to the NE DDoS Protection Policy field and choose a DDoS protection policy from the Select NE DDoS Protection Policy form.

10 Close the IES L3 Access Interface (Edit) form.

11 Close the IES Service (Edit) form.

12 Close the Manage Services form.

Procedure 70-31 To assign an IP address to an IES L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES service and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The VPRN L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Addresses tab.

8 Click on the Create button. The IP Address (Create) form opens.

9 Configure the parameters:

- Address ID
- IP Address
- Prefix Length
- Broadcast Address Format
- EUI-64
- IP Address Preferred

The Broadcast Address Format parameter only appears if the IP Address parameter is set to an IPv4 address.

The EUI-64 and IP Address Preferred parameters only appear if the IP Address parameter is set to an IPv6 address.

10 Click on the OK button. The IP Address (Create) form closes, and a dialog box appears.

11 Click on the OK button. The IES L3 Access Interface (Edit) form reappears with the assigned IP address displayed.

12 Close the IES L3 Access Interface (Edit) form.

13 Close the IES Service (Edit) form.

14 Close the Manage Services form.

Procedure 70-32 To configure bi-directional forwarding detection for an IES L3 access interface



Note — You cannot configure BFD for an interface if BFD is disabled. See chapter 23 for information about enabling and disabling BFD for routing protocols.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES service and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The IES L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the BFD tab. The General tab is displayed.

8 Set the Administration Status to Up.

9 Configure the parameters:

- Transmit Interval
- Receive Interval
- Echo Interval
- Multiplier
- Termination Type
- Operational State Transition Interval
- Inherit from Network Element



Note — If the IPv6 Allowed parameter in Procedure 70-17 is enabled, you can configure the above BFD parameters for IPv6.

10 To view local and remote session peers that are managed by the 5620 SAM, click on the BFD Session tab. A list of BFD current sessions on a router interface or an L3 interface appears.

11 Click on a session. The properties form for the session opens. View the following:

- BFD status
- protocol used
- local address
- remote address
- operational status and statistics

12 Close the form.

13 Close the IES L3 Access Interface (Edit) form.

14 Close the IES Service (Edit) form.

15 Close the Manage Services form.

Procedure 70-33 To configure IPv4 ICMP for an IES L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES service and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The IES L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the ICMP tab.

8 Configure the parameters:

- Mask Reply
- Redirects
- Number of Redirects
- Redirects Time (seconds)
- Unreachables
- Number of Unreachables
- Unreachables Time (seconds)
- TTL Expired
- Number of TTL Expired
- TTL Expired Time (seconds)

9 Close the IES L3 Access Interface (Edit) form.

10 Close the IES Service (Edit) form.

11 Close the Manage Services form.

Procedure 70-34 To configure IPv6 ICMP on an IES L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a IES service and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The IES L3 Access Interface (Edit) form opens with the General tab displayed.

7 Ensure that the IPv6 Allowed parameter is enabled.

8 Click on the ICMPv6 tab.

9 Configure the parameters:

- Redirects
- Number of Redirects
- Redirects Time (seconds)
- Unreachables
- Number of Unreachables
- Unreachables Time (seconds)
- Packet Too Big
- Number of Packet Too Big
- Packet Too Big Time (seconds)
- Param Problem
- Number of Param Problem
- Param Problem Time (seconds)
- Time Exceeded
- Number of Time Exceeded
- Time Exceeded Time (seconds)

10 Close the IES L3 Access Interface (Edit) form.

11 Close the IES Service (Edit) form.

12 Close the Manage Services form.

Procedure 70-35 To configure IPCP for an IES L3 access interface

You can configure IPCP only on the ASAP MDA on the 7750 SR and 7710 SR.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES service and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The IES L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the IPCP tab. The IPCP tab is available when the SAP and port is configured with Null or IPCP encapsulation.

8 Configure the parameters:

- Peer Address
- Primary DNS Address
- Secondary DNS Address



Note — Primary and secondary DNS addresses have similar functionality, although they are assigned independently. When both are present, the primary DNS address is used to resolve address names. If the primary DNS address cannot be used the secondary DNS address is used.

9 Close the IES L3 Access Interface (Edit) form.

10 Close the IES Service (Edit) form.

11 Close the Manage Services form.

Procedure 70-36 To configure ARP for an IES L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES service and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The IES L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the ARP tab. The General tab is displayed.

8 Configure the Timeout (seconds) parameter.

9 Click on the Create button. The Static ARP (Create) form opens.

10 Configure the parameters:

- Unnumbered
- IP Address
- Physical Address

11 Click on the OK button. The Static ARP (Create) form closes.

12 Click on the Proxy ARP tab.

13 Configure the parameters:

- Remote Proxy ARP
- Enable Local Proxy ARP
- Proxy ARP Policy 1
- Proxy ARP Policy 2
- Proxy ARP Policy 3
- Proxy ARP Policy 4
- Proxy ARP Policy 5

14 Close the IES L3 Access Interface (Edit) form.

15 Close the IES Service (Edit) form.

16 Close the Manage Services form.

Procedure 70-37 To configure neighbor discovery on an IES L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES service and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The Site L3 Access Interface (Edit) form opens with the General tab displayed.

7 Ensure that the IPv6 Allowed parameter is enabled.

8 Click on the Neighbor Discovery tab.

9 Click on the Create button. The Neighbor Discovery (Create) form opens.

10 Configure the parameters:

- IP Address
- Physical Address

11 Click on the OK button. A dialog box appears.

12 Click on the OK button. The Neighbor Discovery (Create) form closes, and the IES L3 Access Interface (Create) form refreshes with the neighbor entry.

13 Click on the Proxy ND tab.

14 Configure the parameters:

- Enable Local Proxy
- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5



Note — Do not leave an empty policy parameter between two configured policy parameters. For example, do not configure the Policy 1 and Policy 3 parameters and leave the Policy 2 parameter unconfigured, or the 5620 SAM reorders the policies and moves the policy specified for the Policy 3 parameter to the Policy 2 parameter.

15 Repeat steps 8 to 14 for each neighbor entry you need to create.

16 Close the IES L3 Access Interface (Edit) form.

17 Close the IES Service (Edit) form.

18 Close the Manage Services form.

Procedure 70-38 To configure IPv4 DHCP for an IES L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a IES service and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The IES L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the DHCP tab. The General tab is displayed.

8 Configure the parameters:

- Enable DHCP Relay
- Description
- Trusted
- Lease Populate
- Enable
- Relay Plain BOOTP
- Use ARP

The Lease Populate parameter is configurable when the Enable parameter is enabled.

9 Depending on the type and release of device that you are configuring, the Subscriber Authentication Policy panel is present. Choose a Subscriber Authentication policy, if required. Otherwise, go to step 14.

10 Click on the Select button in the Subscriber Authentication panel to choose a subscriber authentication policy. The Select Subscriber Authentication Policy - DhcpRelayConfiguration form opens.

11 Configure the filter criteria, if required, and click on the Search button.

12 Choose a subscriber authentication policy and click on the OK button. The Select Subscriber Authentication Policy - DhcpRelayConfiguration form closes, and the IES L3 Access Interface (Edit) form refreshes with the subscriber authentication policy name.

13 Configure the parameters:

- Action
- Circuit ID
- Remote ID
- Remote ID String
- Vendor Specific Options
- Vendor String
- IP address
- Use as source
- Relay Unicast Message

The Remote ID String parameter is configurable when the Remote ID is set to Remote ID String.

When the Relay Unicast Message parameter is set to Renew or Release Update Source IP, the GI address parameter can be configured as any local configured address in the same routing instance as the GI address for the DHCP relayed messages. If the Relay Unicast Message parameter is set to None, the GI address is restricted to the IP address configured on the subscriber interface.

14 Click on the Server tab.

15 Configure the parameters:

- Server 1 through Server 8
- Administrative State
- Emulated Server IP Address
- Lease Time
- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time Override

The Number of Days, Number of Hours, Number of Minutes, Number of Seconds, and Lease Time Override parameters are configurable only when the Lease Time parameter is set to Specified Time Period.

16 Close the IES L3 Access Interface (Edit) form.

17 Close the IES Service (Edit) form.

18 Close the Manage Services form.

Procedure 70-39 To configure ATM on an IES L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES service and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The Site L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the ATM tab.



Note — The ATM tab is available when the interface port is an ATM port.

8 Configure the parameters:

- AAL5 Encapsulation
- ATM OAM Alarm Cell Handling
- Periodic ATM OAM Loopback

9 Click on the Select button in the Ingress ATM Policy panel to choose an ingress ATM policy. The Select Ingress ATM Policy - ATM Configuration form opens.

10 Choose an ingress ATM policy and click on the OK button. The Select Ingress ATM Policy - ATM Configuration form closes and the L3 Access Interface form reappears with the ingress ATM policy information displayed.

11 Click on the Select button in the Egress ATM Policy panel to choose an egress ATM policy. The Select Egress ATM Policy - ATM Configuration form opens.

12 Choose an egress ATM policy and click on the OK button. The Select Egress ATM Policy - ATM Configuration form closes and the IES L3 Access Interface (Edit) form reappears with the egress ATM policy information displayed.

13 Close the IES L3 Access Interface (Edit) form.

14 Close the IES Service (Edit) form.

15 Close the Manage Services form.

Procedure 70-40 To create a VRRP instance on an IES L3 access interface for a virtual router

You must know the VRID for an existing virtual router and ensure that the interface is a member of the same subnet as the virtual router.

See chapter 33 for configuration information about VRRP instances and virtual routers.



Note — The following configurations are required for the operation of the IPv6 VRRP instance:

- You can only create an IPv6 VRRP Instance if you enable the IPv6 Allowed parameter on the General tab of the IES L3 Access Interface (Edit) form.
- The Link Local Address on the parent interface must be set to preferred and configured as one of the backup addresses (or same subnet) for the IPv6 VRRP instance. The Admin Link Local Address and Admin Link Local Address Preferred parameters on the General tab of the IES L3 Access Interface (Edit) form must be set accordingly.
- The IPv6 address on the parent interface must be set to preferred to be used as a backup address (on same subnet) for the IPv6 VRRP instance. The IP Address and IP Address Preferred parameters in step 9 of Procedure 70-31 must be set accordingly.
- The Send Advertisement and Use Virtual MAC Address parameters must be enabled in step 9 of Procedure 70-42 for the router advertisement on the parent interface.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES service and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The IES L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the VRRP tab.

8 Click on the Create button. The VRRP Instance (Create) form opens with the General tab displayed.

9 Configure the Virtual Router ID parameter.

10 Perform steps 8 to 15 of Procedure 33-2.



Note — You can use the VR Instances tab to create, modify, and view VR instances.

11 Click on the OK button. The VRRP Instance (Create) closes and the IES L3 Access Interface (Edit) form reappears.

12 Close the IES L3 Access Interface (Edit) form.

13 Close the IES Service (Edit) form.

14 Close the Manage Services form.

Procedure 70-41 To configure anti-spoofing filters for an IES L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES service and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The IES L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Anti-Spoofing tab.

8 Configure the parameters:

- Anti-Spoofing
- ARP Populate

The ARP Populate parameter is configurable when all of the IP addresses of the defined static hosts on the interface are in one of the subnets configured for the interface.

9 Click on the Static Hosts tab to configure static subscriber host entries, if subscriber entries are not available through DHCP lease management.

10 Click on the Create button. The Access Interface Anti-Spoofing Static Host Display (Create) form opens.

11 Configure the parameters:

- IP Address
- MAC Address

Specify at least one IP address or MAC address for each static host. The values specified for the Anti-Spoofing and ARP Populate parameters determine the type of address entry that is required for the static host. For example, when you set the Anti-Spoofing parameter to Source Ip Addr, you must specify at least the IP address for the static host.



Note — You can configure a static host on a SAP only when no static ARP entries exist on the IP interface.

When the ARP Populate parameter is enabled, the IP address of the new static host must be in one of the subnets that is configured for the interface in Procedure 70-31.

12 Click on the Apply button if you need to create additional entries. A dialog box appears. Otherwise, go to step 15.

13 Click on the OK button.

14 Repeat steps 11 to 13 to create additional entries, if required.

15 Click on the OK button. A dialog box appears.

16 Click on the OK button. The Access Interface Anti-Spoofing Static Host Display (Create) form closes and the Static Hosts tab refreshes with the configured static hosts displayed.

17 Close the IES L3 Access Interface (Edit) form.

18 Close the IES Service (Edit) form.

19 Close the Manage Services form.

Procedure 70-42 To configure router advertisement on an IES L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES service and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The IES L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Advertisement tab.

8 Click on the Create button to add a router advertisement entry. The Router Advertisement (Create) form opens.

9 Configure the parameters:

- Send Advertisement
- Min Interval (seconds)
- Reachable Time (milliseconds)
- Managed Address Config
- MTU
- Use Virtual MAC Address
- Max Interval (seconds)
- Retransmit Time (milliseconds)
- Other Stateful Config
- Current Hop Limit
- Lifetime (seconds)

If you are configuring the L3 interface for an IPv6 VRRP instance, then the Send Advertisement and Use Virtual MAC Address parameters must both be enabled.

10 Click on the Prefix tab.

11 Click on the Create button. The Router Advertisement Prefix (Create) form opens.

12 Configure the parameters:

- IPv6 Prefix
- On-Link Determination
- Prefix Length
- Autonomous Address Configuration
- Lifetime (seconds) in Preferred Lifetime panel
- No Expiry in Preferred Lifetime panel
- Lifetime (seconds) in Valid Lifetime panel
- No Expiry in Valid Lifetime panel

13 Click on the OK button. A dialog box appears.

14 Click on the OK button. The Router Advertisement (Create) form reappears.

15 Click on the OK button. A dialog box appears.

16 Click on the OK button. The Router Advertisement (Create) form closes and the IES L3 Access Interface (Edit) form refreshes with the router advertisement entry.

17 Close the IES L3 Access Interface (Edit) form.

18 Close the IES Service (Edit) form.

19 Close the Manage Services form.

Procedure 70-43 To specify queue overrides on an IES L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES service and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The IES L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Override Policy Items tab.



Note — The Override Policy Items tab contains a number of sub-tabs. However, the sub-tabs that are displayed depend on the port type that you have chosen for this interface.

- If you configured a non-HSMDA port, then the Access Ingress Queues, Access Egress Queues, Ingress Policer, and Egress Policer sub-tabs are active.
- If you configured an HSMDA port, then the Access Ingress Queues, Access Egress HSMDA Queues and Ingress Policer sub-tabs are active.

Set the queue overrides, as described in Procedure 43-42.

8 Close the IES L3 Access Interface (Edit) form.

9 Close the IES Service (Edit) form.

10 Close the Manage Services form.

Procedure 70-44 To configure IPv6 DHCP on an IES L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose an IES service and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Site icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The IES L3 Access Interface (Edit) form opens with the General tab displayed.

7 Ensure that the IPv6 Allowed parameter is enabled.

8 Click on the DHCPv6 tab. The General tab is displayed.

9 Configure the parameters:

- Enable DHCPv6 Relay
- Description
- Lease Populate
- Maximum Number of Leases
- Route Populate PD
- Route Populate PD Exclude
- Route Populate NA
- Route Populate TA
- Interface Id Option
- Interface Id String
- Remote ID
- Source IP Address
- Neighbor Resolution
- Prefix Option

10 Click on the Server tab.

11 Configure the Server 1 through Server 8 parameters.

12 Configure the interface name for each DHCPv6 server that you configured in step 11 by clicking on the Select button in the Zone Index panel. The Select Zone Index - DhcpRelayV6Configuration form opens with a list of configured interfaces.

13 Choose an interface and click on the OK button. The Select Zone Index - DhcpRelayV6Configuration list form closes and the IES L3 Access Interface form refreshes with the interface information.

14 Click on the DHCPv6-Prefix tab.

15 Click on the Create button. The DhcpRelayV6PrefixDelegation (Create) form opens.

16 Configure the parameters:

- Prefix Address
- Prefix Length
- Prefix DUID
- Prefix IAID
- Prefix Life Time (seconds)
- Prefix Valid Life Time (seconds)

17 Click on the OK button. A dialog box appears.

18 Click on the OK button. The IES L3 Access Interface (Edit) form reappears.

19 Close the IES L3 Access Interface (Edit) form.

20 Close the IES Service (Edit) form.

21 Close the Manage Services form.

Procedure 70-45 To view the service operational status

The Aggregated Operational State and State Cause indicators on the General tab of the service management form display information about service faults.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose a service and click on the Properties button. The IES Service (Edit) form opens.

4 View the Aggregated Service Site Operational State and State Cause indicators. When the Aggregated Operational State is Down or Partially Down, a check mark beside the appropriate State Cause indicator identifies the type of associated service fault.

5 Click on the appropriate tab to view or edit an object that is identified as faulty by a State Cause indicator.

6 Click on the Faults tab to view the alarms for the object. The Object Alarms tab is displayed.

7 Click on the Aggregated Alarms tab to view the aggregated alarms for the object. The Aggregated Alarms tab is displayed.

8 Close the IES Service (Edit) form.

9 Close the Manage Services form.

Procedure 70-46 To view the service topology

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose an IES and click on the Topology View button. A Topology View dialog box appears.

4 Click on the Yes button to proceed. The Service Topology - map opens.

See chapter 6 for more information about service topology views.

Procedure 70-47 To modify an IES



Caution — Modifying parameters can be service-affecting.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose an IES and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

The following tabs list the service elements that can be individually or collectively selected and configured:

- General tab — displays general customer and service information
- Sites tab — lists the sites that are included in the service
- Interfaces tab — lists the interfaces, such as L3 access, that are included in the service, and allows the creation and configuration of subscriber, group, and redundant interfaces
- SDP Bindings tab — displays the spoke SDP bindings that are associated with the service
- Addresses tab — lists the IP addresses that are associated with the service



Note — You cannot remove an IP address from an interface when the IP address of a static host is defined in the subnet of the interface IP address and the ARP Populate parameter is enabled on the Anti-Spoofing tab.

- Template tab — displays the template used to create the service, if applicable.
- Faults tab — displays the faults associated with the service



Note — Users with the administrator scope of command role can click on the Select button on the Template tab to associate a service template with the service object, if required.

4 Modify the parameters for the service, as required.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button to confirm the action. The IES Service (Edit) form closes, and the Manage Services form reappears.

7 Click on the Close button to close the Manage Services form.

Procedure 70-48 To modify an IES using the topology view

The topology view for a service provides a graphical representation of the various components and their interconnections. You can also use this view to add, modify, or just navigate to service components. This provides an alternative approach to performing these functions from the navigation tree view.

Working from the topology view can expedite the creation of the components, since many of the fields you would ordinarily have to set in the configuration forms will be automatically populated using this approach. The configuration forms can also be accessed directly at any time from this view by right-clicking a component. This allows quick access to conduct more detailed component configuration.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose an IES and click on the Topology View button. The Service Topology map opens.

The remainder of this procedure contains two sub-procedures describing the components that can be created and modified from the topology view. These include:

- Creating a new site. Go to step 4.
- Creating spoke SDP bindings. Go to step 9.

Adding a new site

4 Right-click on any blank space in the service topology map. A contextual menu is displayed. Choose the Create IES Site option.

The Select Network Elements form appears.

5 Select one or more sites to add to the service and click OK. The IES Site (Create) form for the new site is displayed. If you selected more than one site, the IES Site (Multiple Instances) (Create) form for the new sites is displayed.

6 Click on the OK button. The IES Site (Create) (or IES Site (Multiple Instances) (Create)) form closes and the new site (or sites) is displayed on the map.

7 If you need to perform detailed configuration of site properties for the new site, right-click the site icon and select Properties from the contextual menu. The Site (Edit) form opens. See Procedure 70-3 for detailed site configuration information.

8 Go to step 9 if you need to create spoke SDP bindings or go to step 16 to finish.

Creating spoke SDP bindings

9 Select the sites you need to connect in the service topology map and right-click on any one of them. A contextual menu is displayed.



Note — When you create a spoke binding between two sites, the order in which you select them is important. The first site you select will become the source site and the second site will become the destination site. Therefore, it is not recommended that you do a marquee-select in the topology view, since you will not be sure of this hierarchy. Instead, select the sites individually, and hold down the Shift or Ctrl key after your first selection.

10 Select Connect from the contextual menu and choose the Create Spoke SDP Binding option.

The Spoke SDP Binding (Create) form is displayed.



Note — For this function, it is assumed that you clicked on the source site first and then held down the Shift or Ctrl key while right-clicking on the destination site to display the contextual menu.

11 Enable the Auto-Select Transport Tunnel parameter.

12 You can manually configure other parameters here if required, or click on the OK button. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Spoke SDP Binding (Create) form closes and the new binding between the two sites is displayed in the topology view. See Procedure 70-8 for more detailed information on creating and configuring spoke SDP bindings, if required.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. See Chapter 27 for information on how to create the required tunnel. Once the tunnel is created, you can repeat this sub-procedure.

13 Assuming that the spoke SDP binding was successfully created in step 12, select the same two sites again in the topology view, although this time do so in the opposite order that you originally selected them. This will allow you to create a spoke binding for the return tunnel.

14 Right-click on the second site you selected and choose the Create Spoke SDP Binding ... option from the contextual menu. The Spoke SDP Binding (Create) form is displayed.

15 You can manually configure other parameters here if required, or click on the OK button. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Spoke SDP Binding (Create) form closes and the new return binding between the two sites is displayed in the topology view.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. See Chapter 27 for information on how to create the required tunnel. Once the tunnel is created, you can repeat this sub-procedure.

16 Close the Service Topology form.

17 Close the Manage Services form.

Procedure 70-49 To delete an IES



Warning — Deleting a service may result in a service disruption for customers. Consider the implication of deleting the service before proceeding.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 As required, configure the filter criteria to locate the service or range of services to be deleted. A list of services appears at the bottom of the Manage Services form.

3 Choose a service or a range of services from the list.

4 Click on the Delete button. A warning form appears. This form is dynamic based on the priority of the service. Perform one of the following:

- **a** For services with a low priority, go to Step 5.
- **b** For services with a medium priority, configure the "Enter the highest priority of the service being deleted" text field by typing: Medium. Go to Step 5.
- **c** For services with a high priority, configure the "Enter the highest priority of the service being deleted" text field by typing: High. Go to step 5.

5 For all services regardless of how their priority is configured, acknowledge the check box that prompts you confirm that you understand the implications of deleting the service.



Note — If you select multiple services with different priorities, you must enter the highest priority level of selected services before you can delete the services.

6 Click on the Yes button to confirm the action. The service is deleted and removed from the list.

7 Click on the Close button to close the Manage Services form.

71 — VPRN service management

71.1 VPRN service management overview *71-2*

71.2 Sample VPRN service configuration *71-13*

71.3 Sample hub-and-spoke VPRN configuration *71-16*

71.4 Workflow to create a VPRN service *71-20*

71.5 VPRN service management procedures *71-22*

71.1 VPRN service management overview

The 5620 SAM supports the creation of VPRN services using the 7450 ESS in mixed mode, the 7750 SR, the 7710 SR, the 7705 SAR-H, and the 7950 XRS as a PE and provider core (P) router. VPRNs, also called IP VPNs or BGP/MPLS VPNs, are defined in RFC 2547bis. This standard describes a method of forwarding data and distributing routing information across an IP/MPLS service provider core network.

The 5620 SAM does not support the configuration of CE routers or devices.

VPRN services use BGP to exchange the VPRN routes among the PE routers that participate in the VPRN. This is done in a way that ensures that routes from different VPRNs remain distinct and separate, even if two VPRNs have an overlapping address space. PE routers distribute routes to CE routers in the VPRN. Since the CE routers do not peer with each other, there is no overlay visible to the VPRN's routing algorithm. The PE routers use BGP, RIP, OSPFv2, or OSPFv3 as the IGP to distribute internal routes to the CE routers.

Each route in a VPRN service is assigned an MPLS label. When BGP distributes a VPRN route, it also distributes an MPLS label for that route. Before a customer data packet travels across the backbone network, it is encapsulated with the MPLS label that corresponds, in the customer VPRN, to the route that best matches the destination address of the packet.

The MPLS packet is further encapsulated with either another MPLS label or with an IP or GRE tunnel header, so that it gets tunneled across the backbone to the proper PE router. Each route exchanged by the MP-BGP protocol includes an RD that identifies the VPRN association. Thus the backbone core routers do not need to know the VPRN routes.

The 5620 SAM supports end-to-end VPRN configuration using the following methods:

- Tabbed configuration forms with an embedded navigation tree. The navigation tree provides a logical view of the service and acts as a configuration interface.
- Pre-configured template. A user who is assigned the template management role can create a service template. See "Managing templates" in the *5620 SAM Scripts and Templates Developer Guide* for more information about the administrative tasks associated with service templates.

The 5620 SAM supports the configuration in a VPRN of an L3 aggregation mechanism called routed CO. Routed CO uses DHCP relay to manage dynamic subscriber hosts; the network resources for static subscriber hosts are explicitly provisioned. Routed CO supports all residential subscriber management functions of the 5620 SAM. See chapter 65 for more information about residential subscriber management and routed CO.

Routed CO uses a subscriber interface that defines up to 256 subnets. A subscriber interface has child objects called group interfaces. A group interface supports the configuration of multiple SAPs as child objects. A SAP in a group interface supports all residential subscriber management functions. A group interface does not allow the specification of IP subnets or addresses, but inherits the addressing scheme of the parent subscriber interface. The 5620 SAM service topology map displays VPRN subscriber interfaces, group interfaces, and the associated SAPs.

You can configure NAT for dynamic subscriber hosts in a routed CO deployment. NAT implementation in a VPRN service requires a NAT configuration on the VPRN routing instance and a NAT policy that is associated with a subscriber profile. See chapter 24 for information about configuring and deploying NAT, and about configuring a NAT policy. See Procedure 54-18 for information about associating a NAT policy with a subscriber profile. See Procedure 71-3 for information about configuring NAT on a VPRN routing instance.

A VPRN routed CO allows a service provider to resell wholesale carrier services while providing direct DSLAM connectivity. You can create a VPRN service for the retailer and also define subscriber access and configuration information for the retailer network. See Procedure 71-60 for more information on how to define a wholesale and retail VPRN configuration.

IPCP extensions allow you to configure IP addresses and DNS names of remote devices to enable inter-operability with other networks. Specifically setting an IPCP extension is necessary to connect to a mobile service provider network. Routers for mobile services rely on other network routers to provide IP addresses and DNS names (primary and secondary) for a PPP link.

When an IPCP extension is configured, an edge device configured with PPP/MLPPP can signal a far end device.

The General tab of the 5620 SAM service management form displays useful information about the operational state of the service and its sites through the Aggregated Operational State and State Cause indicators.

The 5620 SAM provides OAM tools for service validation and for troubleshooting service and network transport issues. You can run an OAM Validation test suite for the service by clicking on the Validate button, or by clicking on the More Actions button and choosing Validate. Alternatively, you can also perform a One Time Validation. If a check mark appears beside the OAM Validation Failed state cause indicator, the test has failed. The Tested Entity Result tab on the Tests tab displays detailed information about the OAM test result. See chapter 32 for general information about fault management using OAM tools. See chapter 77 for more information about how to configure OAM validation test suites.

The Aggregated Operational State indicator has four possible values: Up, Down, Partially Down, and Unknown. The value is derived from the operational states of the sites that are part of the service, as follows:

- Up—all sites are operationally up
- Partially Down—at least one site is operationally down
- Down—all sites are operationally down
- Unknown—the service has no provisioned sites

When the Aggregated Service Site Operational State is Partially Down or Down, a check mark appears beside the appropriate State Cause indicator to identify the type of fault to the 5620 SAM operator. You can view alarms on the Faults page.

When the Aggregated Operational State is Partially Down or Down, a check mark appears beside the appropriate State Cause indicator to identify the type of fault to the 5620 SAM operator.

When you use the 5620 SAM to create or discover a service, the 5620 SAM assigns a default Service Tier value to the service. The Service Tier parameter value is relevant only in the context of composite service topology views. See chapter 74 for more information about the hierarchical organization of composite services.

Common to all device services, such as VPRN, are policies that are assigned to the service. Policies are defined at a global level and can then be applied to components of the service, such as interfaces or circuits, when the service is configured or modified. The following policies are common to all device services:

- QoS policies define ingress classification, policing, shaping, and marking on the ingress side of the interface. QoS policies are configured using the Access Ingress Policy form, the Access Egress Policy form, and the ATM QoS Policy form.
- Policer control policies to control access ingress policers and access egress policers under a common hierarchy. Policer control policies are configured using the Policer Control Policy Manager.
- Scheduling policies define hierarchical rate limiting and scheduling to govern the scheduling of queues. Scheduler policies are configured using the Scheduler Policy and HSMDA Scheduler Policy forms.
- Port scheduler policies define hierarchical bandwidth allocation and scheduling at the egress port level. Port scheduler policies are configured using the Port Scheduler Policy form.
- Filter policies control network traffic into or out of an interface or circuit based on DHCP, IP, or MAC matching criteria. Filter policies are configured using the ACL IP Filter form, the ACL MAC Filter form, and the DHCP Filter form.
- Accounting policies measure the traffic on a service to ensure proper billing and enforcement of SLAs. Accounting policies are configured using the Accounting Policy form.
- ANCP policies provide status and control information based on port-up and port-down messages and current line rate changes between the edge device and the access node. ANCP policies are configured using the Manage Subscriber Policies form.
- Routing policies control the size and content of the routing tables, the routes that are advertised, and the best route to take to reach a destination. Routing policies are configured using the Routing Policy Manager.

See chapter 42 for more information about policies.

VPRN service routers

A VPRN service consists of CE routers or devices connected to PE routers. PE routers connected to P routers transport data across the IP/MPLS provider core network in service tunnels.

Packets that arrive at an edge 7450 ESS, 7705 SAR-H, 7710 SR, 7750 SR, or 7950 XRS are associated with a VPRN service based on the access interface on which they arrive. An access interface is uniquely identified by the following parameters:

- physical Ethernet port or POS port and channel
- encapsulation type
- encapsulation identifier (if required)

Table 71-1 describes the general functions performed by PE, P, and CE routers in a VPRN. See Figure 71-4 in this chapter for a sample VPRN. See the appropriate hardware services guide for more detailed information about VPRN functionality on the supported managed devices.

Table 71-1 VPRN router functionality

Router type	Functionality
PE	• Are directly connected to PE, CE, and P routers • Learn VPRN routes from CE devices using e-BGP, RIP, OSPFv2 or OSPFv3, or static routes • Maintain a separate routing table, called a VRF, for each service • Exchange multicast VPRN route information with PE routers in other autonomous systems using MP-BGP • Distribute MPLS inner labels using MP-BGP. Before data traverses the IP/MPLS backbone, it is encapsulated with the MPLS label that corresponds, within the VPRN, to the route that best matches the packet's destination address. • Distribute MPLS outer labels using RSVP-TE or LDP. Before the MPLS packet traverses the IP/MPLS backbone, it is further encapsulated with either another MPLS label or with a GRE or MPLS LSP service tunnel header, so that it is tunneled across the backbone to the appropriate PE router. • Use RDs to identify the VPRN associations • Use RTs to determine when a received route is destined for a VPRN • Terminate RFC 2684-encapsulated IPv4 traffic from ATM access network on SAPs
P	• Are directly connected to PE and P routers • Act as transit LSRs • Maintain routes to PE routers and are unaware of specific VPRN routing information
CE	• Are directly connected to PE routers • Provide customer access to the VPRN

Inter-AS connections

You can connect VPRN service sites (or VRFs) on multiple ASs using EBGP. ASs set up mutual connections by exchanging routing information, such as routes and labels. Labeled VPN-IPv4 routes are distributed within an AS on a PE router using IGBP and between ASs using EGBP on an ASBR. The ASBR redistributes VPN-IPv4 routes to an ASBR in another AS, which in turn distributes the routes to PE routers in its own AS or to an ASBR.

When a VPRN inter-AS connection is between two service providers, the ASs must be on private peering points. For an LSP to operate between ASBRs on the AS borders, EBGP peering must be set up between the ASBRs and MPLS label exchange must be supported. Furthermore, an LSP must run from a packet's ingress PE router to its egress PE router.

You can enable inter-AS connections from the BGP settings in Procedure 71-50.

MP-BGP Multicast IPv4

The MP-BGP multicast extension allows for a network topology that supports both multicast and unicast routing. Routes from the unicast routing table can be imported into the multicast routing table, and routes from the multicast routing table can be imported into the unicast routing table. An ASBR can be configured to advertise VPRN routes to peers in other ASs, redistributing unicast routes learned by BGP into MP-BGP routes, and MP-BGP routes into unicast routes. This configuration enables the support of the two sets of routing information.

The MP-BGP multicast extension specifies that BGP can exchange routing information for the multicast IPv4 address family within and between BGP ASs. All configurations entered in a multicast IPv4 address family for a BGP instance affect multicast services and are applied to the multicast routing table. See chapter 23 for more information about the configuration of BGP and the MP-BGP multicast extension.

IPv6 support

The 5620 SAM supports IPv6 configuration of the following functions in VPRN services on the 7710 SR, 7750 SR, and 7950 XRS, and on the 7450 ESS in mixed mode:

- addressing for static routes, L3 access interfaces, and BGP peerings
- router advertisement, ICMP, DHCP, neighbor discovery, and ACL filtering



Note — DHCP is not supported on the 7950 XRS.

To configure IPv6 in a VPRN, you must first enable VPN IPv6 for BGP on the base routing instance of each device that acts as a site in the VPRN.

A customer can use an SNMP utility to manage the IPv6 objects in a VPRN service. SNMP mediation of VPRN objects requires the configuration of a community string on each site in the VPRN, regardless of the IP or SNMP version. SNMPv3 mediation of VPRN IPv6 objects, however, requires the additional configuration of an SNMP context for the VPRN using a CLI. See chapter 10 for information about configuring an SNMPv3 context for a VPRN.

PIM for VPRN

The PIM protocol can be applied to a VPRN service to create a private multicast distribution network. PIM uses an MDT group address to identify multicast traffic for the VPRN instance to prevent flooding of multicast packets to PE devices in the VPRN. VRFs with the same MDT address are members of that group and receive multicast traffic from each other. The MDT address cannot be in the SSM range.

By default, the PIM protocol only uses the information in the unicast routing table to determine the RPF interface. PIM can be configured to use the separate multicast and unicast routing tables built by MP-BGP to perform RPF lookups for multicast-capable sources to build and maintain distribution trees for multicast traffic forwarding. See chapter 23 for more information about configuring PIM to use multicast or unicast routing tables in RPF lookups.

Data-MDT

A data-MDT is a tunnel for high-bandwidth source traffic through the P-network to interested PE routers. Data-MDTs do not broadcast customer multicast traffic to all PE routers in a multicast domain.



Note — Data-MDTs are only supported for VPRN services.

Multicast data transmission from a CE router is typically delivered to all CE routers in the same multicast group. Some CE routers do not require the delivery of a specific multicast stream because there no downstream receivers for the multicast group. You can prune a PE router from the MDT if the router does not deliver multicast traffic to the attached CE routers. This task is beneficial for high-traffic multicast applications.

A data-MDT allows you to configure a traffic threshold in Kb/s. The 5620 SAM signals the data-MDTs when the bandwidth for the SSM group exceeds the configured threshold. The PE router sends an MDT join TLV, at 60 s intervals, over the default MDT to all PE routers. The routers respond with the following actions:

- PE routers that require the SSM group specified in the MDT join TLV; join the data-MDT used by the PE router to transmit the SSM group
- PE routers that do not require the SSM group specified in the MDT join TLV; do not join the data-MDT, pruning the PEs from the MDT

The transmitting PE router switches the multicast stream to the data-MDT after allowing the PE routers to join the data MDT. You can configure the data-MDT delay interval using the 5620 SAM.

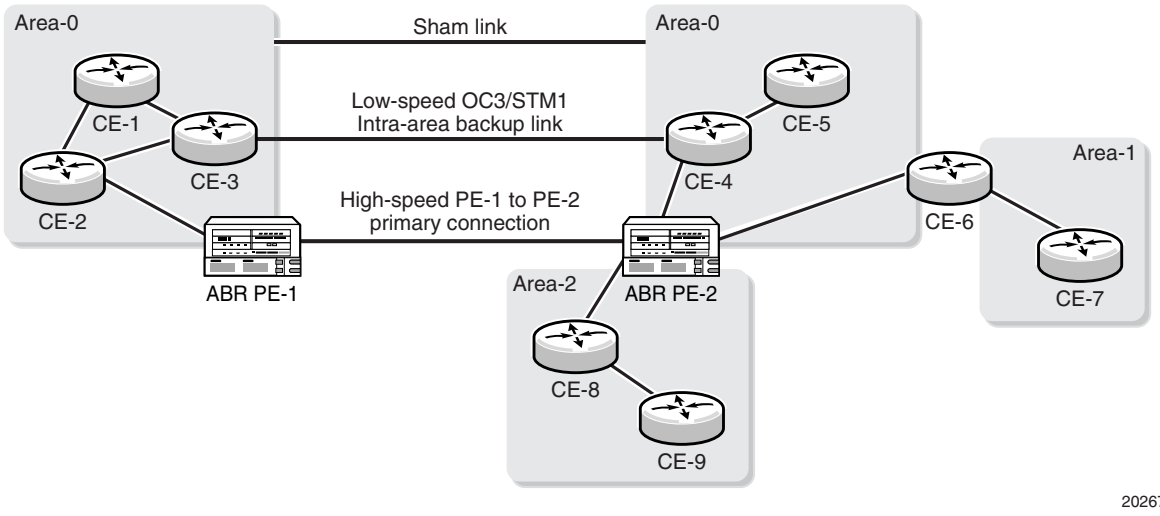
The PE router stops sending the MDT join TLV when the transmission bandwidth no longer exceeds the configured threshold. The PE routers using the data-MDT leave the group and transmission resumes over the default MDT.

OSPF sham link support

You can use the OSPF protocol to connect CE routers to PE routers over an MPLS VPN backbone. This can be useful for customers who subscribe to a VPN service and need to use OSPF as their intra-site routing protocol to exchange routing information between their sites. However, there is a potential configuration issue associated with this approach.

OSPF PE-CE connections assume that the only path between two client sites is across the MPLS VPN backbone. OSPF treats a link through a Layer 3 VPN as an inter-area link. However, other paths between VPN sites may also exist. For example, in Figure 71-1, the link between CE-3 and CE-4 (two CE routers in the same OSPF area) might be a low-speed OC3/STM1 intra-area backup link. OSPF preferentially utilizes intra-area links over inter-area links, and since it establishes an intra-area route connection between CE-3 and CE-4, the potentially high-speed PE-1 to PE-2 primary connection is not utilized.

Figure 71-1 Sham link configuration example



OSPF sham links can be created to resolve this problem. By creating and configuring a sham link as an intra-area link between PE-1 and PE-2, a normal OSPF adjacency is formed, and the link-state database is exchanged across the MPLS VPN. As a result, the desired intra-area connectivity is created between PE-1 and PE-2. In addition, the cost of the CE-3/CE-4 and PE-1/PE-2 links can be managed by the use of a numerical metric. You could then configure the service so that the CE-3/CE-4 link becomes a standby link only in event that the VPN fails.

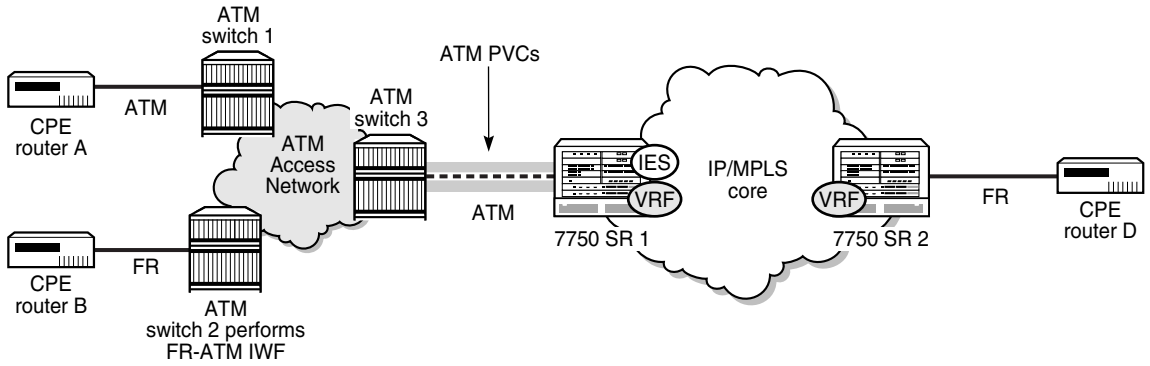
The use of OSPF sham links in VPRNs is supported only on the 7450 ESS, 7710 SR, 7750 SR, and 7950 XRS.

ATM SAP terminations for VPRN

CE routers that have access to an ATM network can connect with a VPRN using ATM SAP terminations on a 7750 SR or 7710 SR. The interconnection between ATM point-to-point and L3 services uses RFC 2684-encapsulated IPv4 traffic over an ATM PVC that terminates on a specially configured SAP. All RFC 2684-encapsulated traffic can be routed over ATM networks, frame relay, or directly through ATM connections.

Figure 71-2 shows how CPE Router A in an ATM network can access L3 IP services, such as a VPRN, using a statically configured ATM PVC on a 7750 SR (SR#1). A SAP is configured on SR #1 to serve a specific VPRN as identified by the VRF. Destination CPE router D can receive RFC 2684-encapsulated traffic over an IP network through a frame relay over 7750 SR 2.

Figure 71-2 ATM SAP network connection to a VPRN



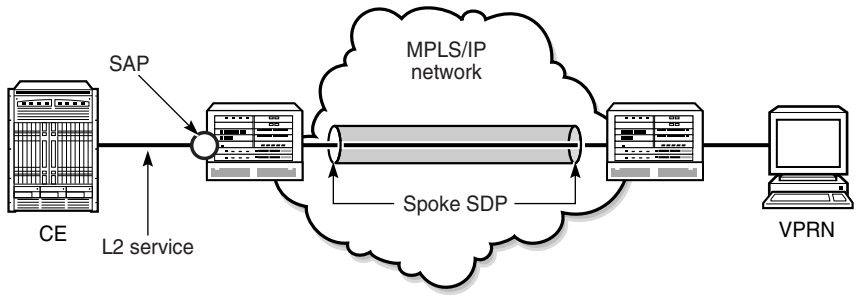
The two connection methods used between ATM and VPRN, which appear in 5620 SAM as AAL5 Encapsulation parameters: LLC/SNAP encapsulation and VC-multiplexing.

Epipe SDP spoke termination on VPRN services

A VLL Epipe service can terminate directly on a VPRN service using an SDP spoke on the 7750 SR, 7450 ESS, 7710 SR, or 7950 XRS. Traffic that terminates on a VPRN service is identified by the interface ID of the SDP on the L2 access router and the VC ID label in the service packet. All routing protocols supported by VPRN are also supported for spoke SDP termination.

Figure 71-3 shows a spoke SDP terminating directly on a VPRN. The spoke SDP could be tied to an Epipe or VPLS. No configuration is required for the CE-to-PE connection on the SAP.

Figure 71-3 SDP spoke termination on an L2 service



Routed CO dual homing using SRRP

Subscriber Router Redundancy Protocol (SRRP) allows two separate connections to an access NE such as DSLAM to operate in an active/standby configuration similar to the way in which VRRP interfaces operate. SRRP is a collection of functions and messaging protocols that allows a system to create a set of redundant gateway IP addresses that are shared by a local and remote NE.

Each SRRP instance is created within the context of a subscriber group IP interface and is identified by a unique SRRP instance ID, which must be unique within the NE. This SRRP instance controls the redundant routing for all subscriber subnets configured or associated with the group interface. One SRRP instance is supported for each group interface and the SRRP ID must be the same as the SRRP instance ID on the group IP interface on the redundant NE.

A subscriber subnet redundant gateway IP host address is assigned at the subscriber IP interface level and is used for each SRRP instance associated with the subscriber subnet. The redundant IP host address must be configured for a subscriber subnet before it can be associated with an SRRP instance.

When SRRP is active on a group interface, the SRRP instance advertises to a remote NE using in-band messaging on the group-interface SAPs and out-of-band messaging on the group-interface redundant interface. If the remote NE uses the same SRRP instance ID, one NE enters a master state, while the other NE enters a backup state. Since the NEs share a common SRRP gateway MAC address (used for the SRRP gateway IP address and for proxy ARP functions), either NE can act as the default gateway for the attached subscriber hosts. This functionality helps to preserve subscriber QoS enforcement. The master state allows routing to and from the subscriber hosts associated with the group IP interface. The backup state stops ingress forwarding for packets destined to the SRRP gateway MAC and causes all packets destined to subscriber hosts on the group IP interface to be forwarded to a redundant IP interface associated with the group IP interface.

Normally, when anti-spoofing is enabled on a group-interface SAP, the SAP drops SRRP packets because they do not contain a subscriber MAC or IP address. However, you can use a configuration option to enable anti-spoofing for subscriber hosts on a group-interface SAP that participates in SRRP advertisements.

The underlying mechanism that controls state transitions is based on a dynamic priority level that an SRRP instance maintains. The SRRP instance with the highest priority level assumes the master operating state. An SRRP instance with a higher current priority level always preempts an SRRP instance with a lower priority level. If the priority levels are equal, the SRRP instance with the lowest source SRRP host IP address assumes the master state. The local SRRP instance priority may also be controlled by associating the instance with an existing VRRP policy.

To prevent a flood of AccessInterfaceDown alarms that an SRRP fault or link failure may generate for LAG-based MSAPs, the 5620 SAM performs alarm suppression. See chapter 65 for more information.

The redundant IP interface is a special interface that connects two systems with one or more common SRRP instances. The interface is configured with a /31 address and a spoke SDP binding, creating an Ethernet pseudowire shortcut between the redundant NEs. When the SRRP instance is in backup state, the group interface associated with this instance is not allowed to forward or route traffic downstream towards the subscriber. As a result of this, the packets are shunted across the redundant interface so that the active group interface does the forwarding or routing.

If the redundant IP interface goes down, the system allows the group IP interfaces associated with the down interface to forward locally downstream, when they are in the backup SRRP state. While forwarding downstream in the backup state, the system uses the MAC address associated with the group IP interface, not the SRRP redundant gateway MAC address.

SRRP is supported on the 7450 ESS in mixed mode, 7710 SR and 7750 SR.

DoS protection

To protect a VPRN from a high incoming packet rate that characterizes a DoS attack, you can use the 5620 SAM to create DoS protection policies for the VPRN L3 access interfaces. A DoS protection policy limits the number of control-plane packets that an interface receives each second, and optionally logs a violation notification if a policy limit is exceeded. You can use the NE System Security form to view the violations for a specific NE.

You can configure a DoS protection policy to control the following on a VPRN L3 access interface:

- the control-plane packet arrival rate per subscriber host on the interface
- the overall control-plane packet arrival rate for the interface
- whether an NE sends a notification trap if a policy limit is exceeded

Each VPRN L3 access interface on an NE that supports DoS protection is automatically assigned a default DoS protection policy. This default policy limits only the overall packet arrival rate for the interface, and cannot be deleted or modified. See "To configure an NE DoS protection policy" in the *5620 SAM System Administrator Guide* for information about creating a DoS protection policy.

DDoS protection

To protect a VPRN from a high incoming packet rate that characterizes a DDoS attack, you can use the 5620 SAM to configure TMS interfaces to route malicious traffic through the ISA-TMS MDA where the malicious traffic is cleaned before being released to the network.

The TMS interface on a VPRN consists of three VPRNs as follows:

- The management VPRN communicates with the TMS server to determine whether incoming packets are malicious. Configuration of this VPRN is optional.
- The Off-Ramp VPRN receives the malicious traffic and routes it through the ISA-TMS MDA where the traffic is scrubbed. Configuration of this VPRN is optional.
- The On-Ramp VPRN returns the cleaned traffic to the network. Configuration of this VPRN is mandatory.

See Procedure 71-64 for information about creating a TMS interface.

You can configure a DDoS protection policy on a VPRN group interface SAP, network interface, or L3 access interface. See "To configure an NE DDoS protection policy" in the *5620 SAM System Administrator Guide* for more information.

Local DHCP servers

A local DHCP server can be associated with an L3 access interface on a VPRN service. See section 65.4.

Local user database

A local user database can be associated with a local DHCP server and PPPoE configurations on group interfaces. See section 65.4.

PPPoE protocol on VPRN services

A VPRN service can be configured to run PPPoE protocol. PPPoE is used in subscriber networks to encapsulate PPP frames inside Ethernet frames. PPPoE combines the point-to-point protocol used with DSL sessions with the Ethernet protocol used to support multiple subscribers in a local area network. From the group interface configuration form you can assign a PPPoE policy and a local user database to authenticate PPPoE subscribers.

PPPoE termination in a business VPRN environment is also supported. This ability targets applications such as PPPoE VPRN with IP overlap, where there are two participants in the service:

- The “Wholesale VPRN”, which is a VPRN that provides access to the SAP.
- The “Retail VPRN”, which is a business VPRN that routes the packets belonging to the PPPoE sessions terminating in it. The Retail VPRNs may have overlapping IP addresses.

In this configuration, the PPPoE subscriber host terminates in a Retail VPRN and provides a routed path to the customer site. The VPRN service-id that carries it is determined by the service configuration, specifically:

- If a local user database is used, the Retail Service ID property that you specify in the PPPoE host configuration provides a reference to the VPRN service-id that should be used.
- If RADIUS is used for authentication, the retailer service-id is provided by an Alcatel-Lucent VSA.
- If MSAP is used, the SAP is created in the wholesale VPRN using the information from RADIUS.

The PPPoE session is negotiated with the parameters defined by the Wholesale VPRN interface. Since the IP address space of the subscriber management host may overlap between VPRN services, the node anti-spoofs the packets at access ingress with the session-id.

L2TP on VPRN services

The 5620 SAM supports the configuration of L2TP on a 7710 SR, 7750 SR, or 7950 XRS, and on the 7450 ESS in mixed mode. L2TP is a session-layer protocol that extends the PPP model by allowing L2 and PPP endpoints to reside on different devices that are interconnected by a PSN. L2TP extends the PPP sessions between the CPE and PPP/L2TP termination points on the L2TP network server (LNS), via an intermediate L2TP access concentrator (LAC). The LAC is the initiator of session-generated L2TP tunnels; the LNS is the server that waits for new tunnels. Manually configured and initiated L2TP tunnels can be initiated or stopped from either the LNS or LAC.

At least one ISA-LNS group must be configured for the LNS NE.

On an LNS NE, L2TP destinations configured for L2TP tunnel profiles can include the following:

- loopback L3 access interfaces for a VPRN or IES service
- loopback interfaces configured for a base routing instance

See chapter 14 for more information about ISA-LNS groups. See Procedure 14-6 for information about how to create and configure an ISA-LNS group. See chapter 23 for more information about L2TP.

See Procedure 71-50 for information about enabling L2TP on a VPRN router instance site. See Procedure 71-60 for information about configuring a VPRN group interface to terminate LNS PPP sessions.

IPsec

You can configure a VPRN with a tunnel interface for secure and encrypted tunneling between sites. An IPsec VPRN allows you to share secure and encrypted VPN traffic among multiple sites.

IPsec VPRN services include:

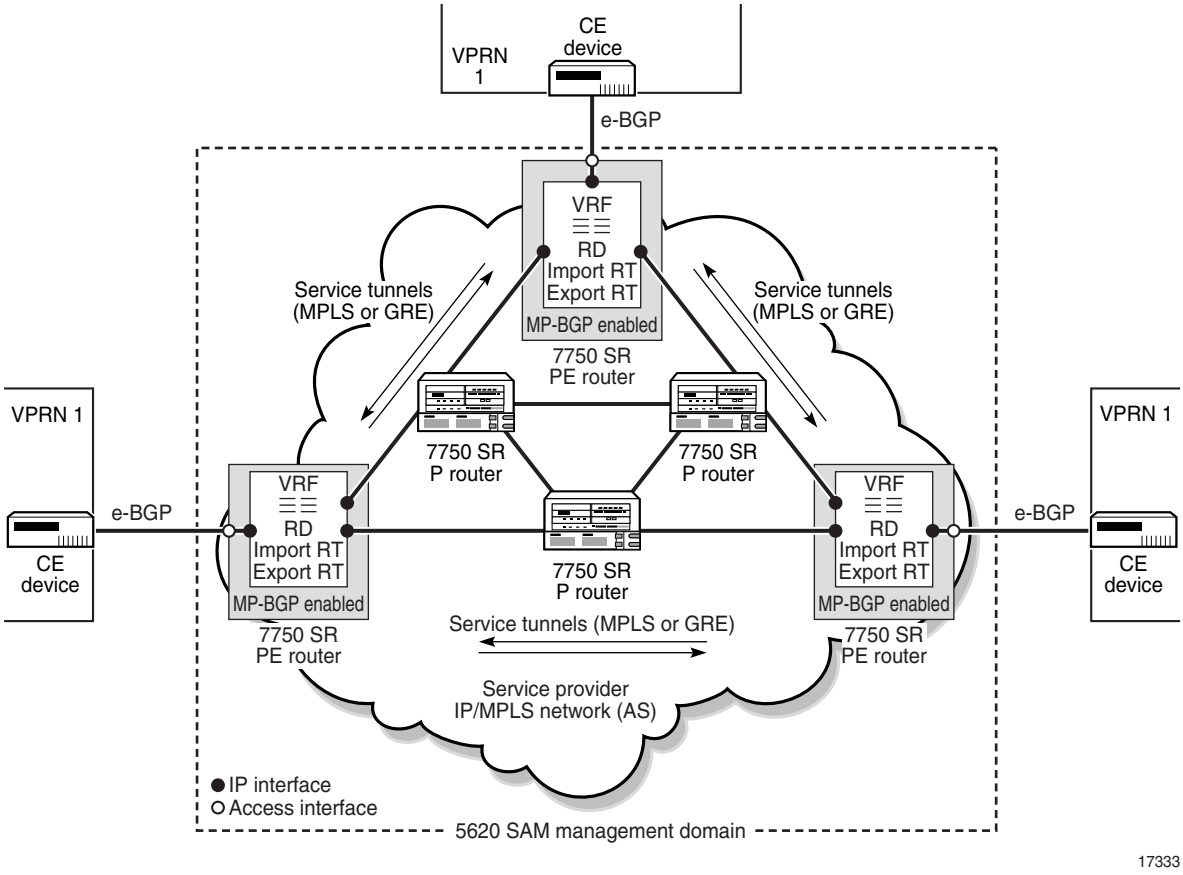
- NAT traversal
- DES, 3DES, AES-128, AES-192 and AES-256 encryption methods
- HMAC-MD5 and HMAC-SHA1 authentication and hashing methods
- Diffie-Hellman key generation algorithms
- Pre-shared keys and IKE shared secret with PFS key management authentication methods

See chapter 29 for more information about IPsec configuration.

71.2 Sample VPRN service configuration

Figure 71-4 shows a sample VPRN service configuration.

Figure 71-4 Sample VPRN Configuration



Assuming the core IP/MPLS or GRE network is already configured, Table 71-2 lists the high-level tasks that are required to configure the sample VPRN service.

Table 71-2 Sample VPRN service configuration

Task	Description

1. Configure policies as required	Policies should be configured before you create a service. Participation in policies is defined when you configure or modify resources, such as access interfaces or circuits, during service creation or modification. The following key policies can be applied to resources that are part of a VPRN.
	• Routing policies.
	  • Choose Policies→Routing→Statement to open the routing policy-statements form.
	  • Choose Policies→Routing→Prefix List to open the routing policy-prefix lists form.
	  • Choose Policies→Routing→Community to open the routing policy-communities form.
	  • Choose Policies→Routing→Damping to open the routing policy-dampings form.
	  • Choose Policies→Routing→AS Path to open the routing policy-AS paths form.
	• Access ingress and egress interface policies. Choose Policies→QoS→SROS QoS→Access Ingress or Access Egress, then the name of the form you need to configure, to open these forms.
	• Scheduler policies. Choose Policies→QoS→SROS QoS→Scheduler, then the name of the form you need to configure, to open the scheduler policy forms.
	• ACL IP filter policies. Choose Policies→Filter→ACL IP Filter to open the ACL form.
	• Accounting policy. Choose Tools→Statistics→Accounting Policies to open the accounting policy form.
	• ANCP policy. Choose Policies→Residential Subscriber to open the Manage Subscriber Policies form.

2. Configure ports as access ports for use in the service	Right-click on a port from the equipment navigation tree and choose Properties. Specify the port as an access port and optionally specify an encapsulation type.
3. Configure service tunnels as required	Choose Manage→Service Tunnels to create service tunnels. Service tunnels carry service traffic between edge-managed routers by circuits aggregated in unidirectional service tunnels. Circuits can be associated with service tunnels during service configuration.
4. Configure MP-BGP for PE-to-PE routing.	Perform the following steps. See chapter 23 for more information about protocol configuration. • Right-click on a router instance in the Routing view of the network navigation tree and choose Properties. In the Properties form that opens, click on the Routing tab, and select the BGP check mark box on the Protocols tab. • Right-click on the BGP instance in the Routing view of the network navigation tree and choose Properties. In the Properties form that opens, click on the VPN tab and enable VPN IPv4 or VPN IPv6 as required. Enable Multicast IPv4 or Multicast IPv6 to apply a multicast definition to this BGP routing instance. Click on the Behavior tab and set the Enable Inter AS VPRN parameter to true. • Right-click on the BGP Peer Group instance in the Routing view of the network navigation tree and choose Create Peer. In the Peer form that opens, configure the Peer Address and other parameters.
5. Create and configure customers	Choose Manage→Service→Customers to open the customer manager form and create a customer.

(1 of 2)

Task	Description

6. Create and configure VPRN 1.	Ensure that the operator creating the service has Service Mgmt and Interface Mgmt user group privileges. See "5620 SAM user security tasks" in the *5620 SAM System Administrator Guide* for more information about user and user group privileges.
	Choose Create→Service→VPRN. Use the tabbed form and embedded navigation tree to configure the service. You configure the following key elements when you configure VPRN 1.
	• Specify the newly created customer as the customer for the VPRN 1.
	• Specify and configure the VPRN service sites. Perform the following for each VRF:
	  • Configure autobinding to specify that the service is automatically bound to service tunnels.
	  • Configure routing properties.
	  • Configure the route distinguisher.
	  • Configure VRF targets.
	  • Configure import and export route targets.
	  • Configure import and export routing policies.
	  • Configure BGP on the PE VPRN sites for PE-to-CE routing. See chapter 23 for information about routing protocol configuration.
	  • If required, configure a GSMP group and a GSMP group neighbor
	  • If required, configure PIM to create a multicast domain within the VPRN.
	  • If required, configure the RPF Lookup Sequence parameter to specify which routing tables PIM uses for standard multicast and unicast RPF lookups.
	  • If required, configure an override source IP address or L3 interface used by IP applications to communicate with the site.
	• Create and configure an access interface on each VPRN service site.
	  • Configure general parameters such as a name, ID, and MAC address.
	  • Assign an application profile, if required.
	  • Assign an AA transit IP or transit prefix policy, if required.
	  • Specify a port that is in access or hybrid mode.
	  • Assign ingress and egress QoS policies as required.
	  • Assign an aggregation scheduler for traffic rate limiting across the card or port, if required. Otherwise, assign ingress and egress scheduler policies.
	  • Assign ACL filter policies as required.
	  • Assign an accounting policy, if required.
	  • Specify a local DHCP server, if required.
	  • Specify a ToD suite, if required.
	  • Configure subscriber management parameters, if required.
	  • Specify a DoS protection policy, if required.
	  • Configure a local IP address.
	  • Configure the ARP timeout and proxy ARP settings, if required.
	  • Configure ICMP parameters, if required.
	  • Configure IPCP parameters, if required.
	  • Configure DHCP parameters, if required.
	  • Configure VRRP parameters, if required.
	  • Configure anti-spoofing parameters, if required.
	  • Configure VRRP parameters, if required.
	  • Configure router advertisement parameters.
	  • Configure ANCP parameters, if required.

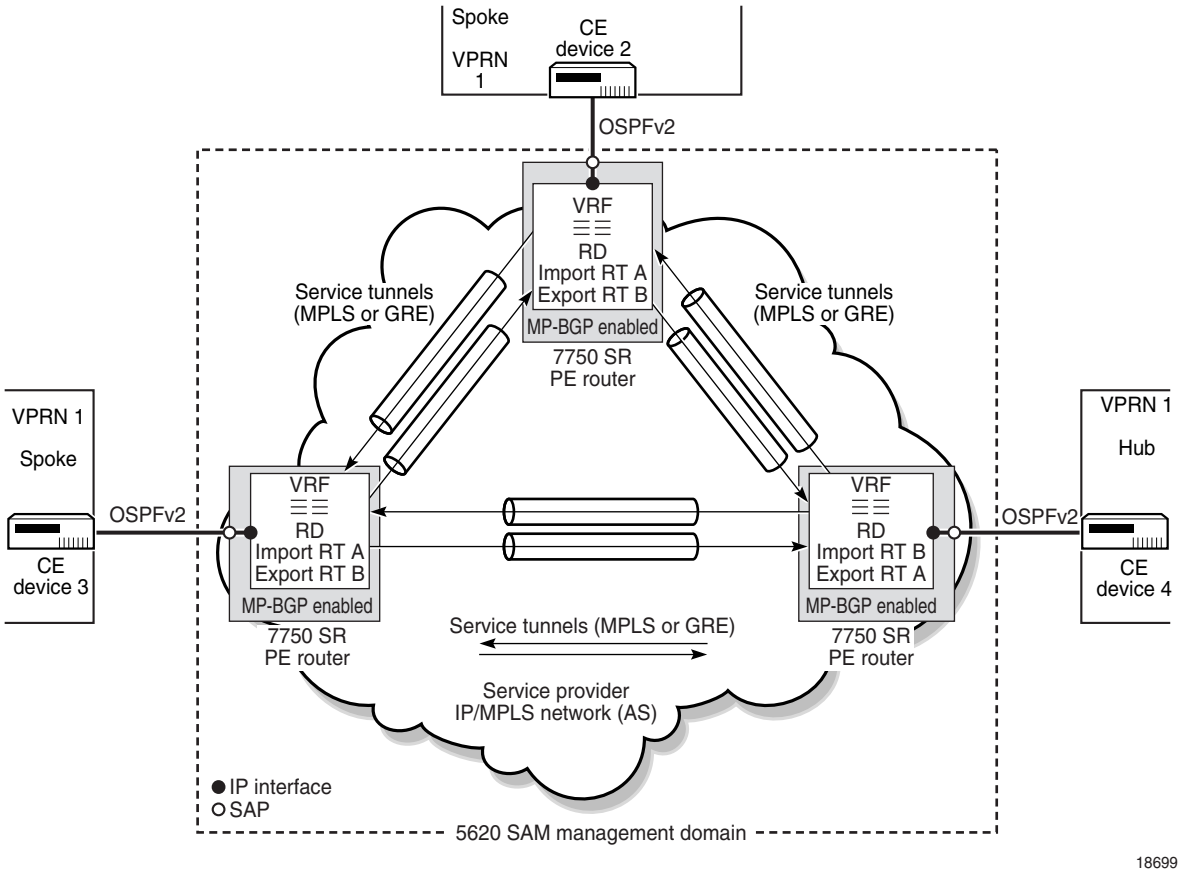
(2 of 2)

71.3 Sample hub-and-spoke VPRN configuration

In a hub-and-spoke VPRN, the majority of the traffic is exchanged between the hub (for example, headquarters) and spoke sites (for example, branches). Traffic between spoke sites passes through the hub site. Spoke sites advertise their routes to the hub site, which in turn advertises these routes to the other spoke sites.

Figure 71-5 shows a sample hub-and-spoke VPRN service configuration. Your configuration will vary depending on your network requirements.

Figure 71-5 Sample hub-and-spoke VPRN Configuration



Assuming the core IP/MPLS or GRE network is already configured, Table 71-3 lists the high-level tasks that are required to configure this sample hub-and-spoke VPRN service.

Table 71-3 Sample hub-and-spoke VPRN service configuration

Task	Description

1. Configure policies as required	Policies should be configured before you create a service. Participation in policies is defined when you configure or modify resources, such as access interfaces or circuits, during service creation or modification. The following key policies can be applied to resources that are part of a VPRN.
	• Routing policies.
	  • Choose Policies→Routing→Statement to open the routing policy-statements form.
	  • Choose Policies→Routing→Prefix List to open the routing policy-prefix lists form.
	  • Choose Policies→Routing→Community to open the routing policy-communities form.
	  • Choose Policies→Routing→Damping to open the routing policy-dampings form.
	  • Choose Policies→Routing→AS Path to open the routing policy-AS paths form.
	• Access ingress and egress interface policies. Choose Policies→QoS→SROS QoS→Access Ingress or Access Egress, then the name of the form you need to configure, to open these forms.
	• Scheduler policies. Choose Policies→QoS→SROS QoS→Scheduler, then the name of the form you need to configure, to open the scheduler policy forms.
	• ACL IP filter policies. Choose Policies→Filter→ACL IP Filter to open the ACL form.
	• Accounting policy. Choose Tools→Statistics→Accounting Policies to open the accounting policy form.
	• ANCP policy. Choose Policies→Residential Subscriber to open the Manage Subscriber Policies form.
	• DoS protection policy. Choose Administration→Security→NE DoS Protection to open the NE DoS protection form.

2. Configure ports as access ports for use in the service	Right-click on a port in the equipment navigation tree and choose Properties. Specify the port as an access port and specify an encapsulation type, if required.
3. Configure service tunnels as required	Choose Manage→Service Tunnels to create service tunnels. Service tunnels carry service traffic between edge-managed routers by circuits aggregated in unidirectional service tunnels. Circuits can be associated with service tunnels during service configuration.
4. Configure MP-BGP for PE-to-PE routing.	Perform the following steps. See chapter 23 for more information about protocol configuration. • Right-click on a router instance in the Routing view of the network navigation tree and choose Properties. In the Properties form that opens, click on the Routing tab and select the BGP check mark box on the Protocols tab. • Right-click on the BGP instance in the Routing view of the network navigation tree and choose Properties. In the Properties form that opens, click on the VPN tab and enable VPN IPv4 or VPN IPv6 as required. Enable Multicast IPv4 or Multicast IPv6 to apply a multicast definition to this BGP routing instance. Click on the Behavior tab and set the Enable Inter AS VPRN parameter to true. • Right-click on the BGP Peer Group instance in the Routing view of the network navigation tree and choose Create Peer. In the Peer form that opens, configure the Peer Address and other parameters.
5. Create and configure customers	Choose Manage→Service→Customers to open the customer manager form and create a customer.

(1 of 2)

Task	Description

6. Create and configure VPRN 1	Ensure that the operator creating the service has Service Mgmt and Interface Mgmt user group privileges. See "5620 SAM user security tasks" in the *5620 SAM System Administrator Guide* for more information about user and user group privileges.
	Choose Create→Service→VPRN. Use the tabbed form and embedded navigation tree to configure the service. You configure the following key elements when you configure VPRN 1.
	• Specify the newly created customer as the customer for the VPRN 1.
	• Specify and configure the sites for VPRN 1. For each VRF:
	  • Configure autobinding to specify that the service is automatically bound to service tunnels.
	  • Configure routing properties.
	  • Configure the route distinguisher.
	  • Configure VRF targets.
	  • Configure import and export route targets.
	  • Configure import and export routing policies.
	  • Configure BGP on the PE VPRN sites for PE-to-CE routing. See chapter 23 for information about routing protocol configuration.
	  • Configure other routing protocols on the sites, as required.
	  • If required, configure a GSMP group and a GSMP group neighbor
	  • If required, configure PIM to create a multicast domain within the VPRN.
	  • If required, configure the RPF Lookup Sequence parameter to specify which routing tables PIM uses for standard multicast and unicast RPF lookups. See chapter 23 for more information about protocol configuration.
	  • If required, configure an override source IP address or L3 interface used by IP applications to communicate with the site.
	• Create and configure one or more access interface on each VPRN service site.
	  • Configure general parameters such as a name, ID, and MAC address.
	  • Assign an application profile, if required.
	  • Assign an AA transit IP or transit IP policy, if required.
	  • Specify a port that is in access or hybrid mode.
	  • Assign ingress and egress QoS policies as required.
	  • Assign an aggregation scheduler for traffic rate limiting across the card or port, if required. Otherwise, assign ingress and egress scheduler policies.
	  • Assign ACL filter policies as required.
	  • Assign an accounting policy, if required.
	  • Specify a local DHCP server, if required.
	  • Specify a ToD suite, if required.
	  • Configure subscriber management parameters, if required.
	  • Specify a DoS protection policy, if required.
	  • Configure a local IP address.
	  • Configure the ARP timeout and proxy ARP settings, if required.
	  • Configure ICMP parameters, if required.
	  • Configure IPCP parameters, if required.
	  • Configure DHCP parameters, if required.
	  • Configure VRRP parameters, if required.
	  • Configure anti-spoofing parameters, if required.
	  • Configure VRRP parameters, if required.
	  • Configure router advertisement parameters.
	  • Configure ANCP parameters, if required.

(2 of 2)

71.4 Workflow to create a VPRN service

The following workflow lists the high-level steps required to create a VPRN service. As a prerequisite for creating a VPRN service, this workflow assumes the following:

- a group or customer with the required user access privileges has been configured.
- the IP or IP/MPLS core network exists.
- any required service tunnels are created including the static or dynamic LSP required to create the service tunnel; see Procedure 27-1 for more information.
- the access ports for the service are created; see chapter 16 for more information.
- any required pre-defined routing, QoS, scheduling, filter, accounting, and time of day suite policies are created; see chapter 42 for more information. You do not have to create pre-defined policies if policies are created on a per-service basis.
- any required MP-BGP for PE-to-PE routing is configured; see chapter 23 for more information about protocol configuration.

1 Create the VPRN service; see Procedure 71-1 for more information.

i Choose a customer to associate with the VPRN service.

ii Define the general properties for the VPRN service.

iii Configure NAT on the VPRN Site.

iv Configure multicasting for the VPRN service, if required.

v Enable one or more routing protocols on the VPRN site.

vi Configure a GSMP group on the site, if required.

vii Configure a local DHCPv4 server or local DHCPv6 server on the VPRN site, if required. See Procedures 71-14 and 71-15.

viii Turn up the VPRN service.

2 As required, configure AA reporting to the 5670 RAM; see Procedure 71-2 for more information.

3 As required, create a VPRN site; see Procedure 71-3 for more information.

4 As required, perform one or more of the following on a VPRN site.

a Configure NAT on the VPRN site; see Procedure 24-3 for more information.

b Configure RADIUS servers on the VPRN site; see Procedure 22-7 for more information.

c Configure RADIUS proxy servers on the VPRN site; see Procedure 22-8 for more information.

d Configure NTP on the VPRN site; see Procedure 71-23 for more information.

e create an L3 access interface for the VPRN site; see Procedure 71-22 for more information

f create an L3 network interface for the VPRN site; see Procedure 71-48 for more information

g add a GNE site and GNE service interfaces to an existing VPRN service; see Procedure 71-49 for more information

h configure BGP, OSPFv2, OSPFv3, PIM, IGMP, RIP or L2TP in the VPRN routing instance; see Procedure 71-50 for more information

i configure IGMP on a VPRN routing instance; see Procedure 71-52 for more information

j add a Global Route Table to a VPRN site; see Procedure 71-53 for more information

k add a PIM interface to the VPRN; see Procedure 71-54 for more information

l add an IGMP interface to the VPRN; see Procedure 71-55 for more information

m create a VPRN spoke SDP binding; see Procedure 71-56 for more information

n create an L2 SDP spoke termination on a VPRN service; see Procedure 71-57 for more information

o add a subscriber interface to the VPRN; see Procedure 71-59 for more information

p add a group interface to the VPRN (only the 7450 ESS in mixed mode, 7710 SR and 7750 SR support the configuration of a group interface in a VPRN); see Procedure 71-60 for more information

q collect and view PPP ATM SAP statistics and information for a VPRN group interface; see Procedure 71-61 for more information

r configure WLAN GW for a VPRN group interface; see Procedure 71-62 for more information

s add an IP mirror interface to the VPRN; see Procedure 71-63 for more information

t add a TMS interface to the VPRN; see Procedure 71-64 for more information

u to implement dual homing using SRRP; see Procedure 71-65 for more information

v create an intra-area OSPF sham link between two VPRN sites; see Procedure 71-66 for more information

w add a tunnel interface to a VPRN; see Procedure 29-6 for more information

x Create and enable a video interface for the VPRN, if required. See Procedure See Procedure 30-1 for more information

5 As required, run an OAM validation test for a VPRN. See Procedure 71-67 for more information.

6 As required, view VPRN service information:

a view the service topology map associated with a VPRN service; see Procedure 71-68 for more information

b view the VPRN service operational status; see Procedure 71-69 for more information

c view the DHCPv6 prefixes that the server has given out; see Procedure 71-70 for more information

d view the lease not owner and pool unknown log events for local DHCPv6 servers; see Procedure 71-71 for more information

7 As required, modify a VPRN service:

a using the Manage Services form; see Procedure 71-72 for more information

b using the topology view; see Procedure 71-73 for more information

8 As required, delete a VPRN service. See Procedure 71-74 for more information.

71.5 VPRN service management procedures

Use the following procedures to perform VPRN creation and management tasks.

Procedure 71-1 To create a VPRN service

1 Choose Create→Service→VPRN from the 5620 SAM main menu. The VPRN Services (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the VPRN. The Select Customer - VPRN Service form opens.

3 Choose a customer for the VPRN and click on the OK button. The Select Customer - VPRN Service form closes and the VPRN Services (Create) form refreshes with the customer information.

4 Configure the parameters:

- Service ID
- Auto-Assign ID
- SVC Mgr Service ID
- Service Name
- Description
- Service Tier
- Service Priority
- Administrative State
- Automatic SDP Binding Creation
- IP Address Overlap Avoidance Enabled
- Profile Name
- Current OLC State
- Revert OLC State

The SVC Mgr Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.

The Profile Name parameter is configurable when the Automatic SDP Binding Creation parameter is enabled.

The Current OLC State and Revert OLC State parameters are configurable when you click on the Apply button.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button to confirm the action. The VPRN Service (Create) form closes.

Procedure 71-2 To configure AA reporting to the 5670 RAM

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service.

4 Click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

5 Click on the Application Assurance tab. The 5670 RAM Parameters tab is displayed.

6 Configure the parameters:

- Enable Application Performance Reporting
- Report Customer Name
- Number Of IP Detail Addresses

7 As required, perform Procedure 76-19 to configure a custom DCP subnet group.

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button to confirm the action. The VPRN Service (Create) form closes.

Procedure 71-3 To configure a VPRN site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Perform one of the following.

a Create a VPRN site:

i On the navigation tree, right-click on the Site icon and choose Create VPRN Site. The Select Network Elements - VPRN Service form opens with a list of available sites displayed.

ii Choose a site and click on the OK button. The VPRN Site (Create) form opens with the General tab displayed.

b Configure an existing VPRN site:

i Expand the Sites icon in the service navigation tree.

ii Right-click on a Routing Instance icon and choose Properties from the contextual menu. The VPRN Site (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State
- GSMP Administrative State
- Tunnel Fault Notification
- Current OLC State
- Revert OLC State

Tunnel Fault Notification is configurable on sites where the device has ports configured in access or hybrid mode with QinQ encapsulation.

If you are configuring a tunnel facility MEP, Tunnel Fault Notification must be set to Accept, in order to receive the fault notification from the tunnel facility MEP.

6 Configure the NE-specific parameters, as listed in Table 71-4.

Table 71-4 NE-specific parameters

NE	Parameters	Dependencies	Go To
7750 SR-c4, 7750 SR-7, 7750 SR-12, 7450 ESS, 7710 SR, 7950 XRS	• Enable Hash Label	—	—
7750 SR-7, 7750 SR-12, 7450 ESS	• Reassembly Group	—	—

7 Click on the OK button. A dialog box appears.

8 Click on the OK button. The Site (Create) form closes, and the VPRN Service (Edit) form reappears with the new site information displayed in the service navigation tree.

9 Click on the OK button. A dialog box appears.

10 Click on the Yes button to confirm the action. The VPRN Service (Edit) form closes.

Procedure 71-4 To configure an SNMP community for mediating the IPv6 objects on a VPRN site

If the VPRN site is to support IPv6 addressing (for router advertisement or neighbor discovery) or VRRP objects, perform the following procedure to configure an SNMP community for mediating the IPv6 objects.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Right-click on a Routing Instance icon and choose Properties from the contextual menu. The VPRN Site (Edit) form opens with the General tab displayed.

6 Click on the SNMP Community tab.

7 Click on the Create button. The SNMP Community (Create) form opens.

8 Configure the SNMP Community String parameter.

9 Click on the OK button. The SNMP community string entry is displayed on the Site (Edit) form and a dialog box appears.

10 Click on the OK button. The SNMP Community (Create) form closes.



Note — When the 5620 SAM uses SNMPv2 for device mediation, you must configure one and only one SNMP community string for the VPRN site. Otherwise, there is no mediation of the VPRN IPv6 objects on the site, and the 5620 SAM raises an alarm. The alarm is cleared and mediation resumes after the configuration is modified so that exactly one SNMP community string is associated with the VPRN site.

11 Click on the OK button to close the VPRN Site (Edit) form.

12 Close the VPRN Service (Edit) form.

13 Close the Manage Services form.

Procedure 71-5 To configure an MVPN VRF instance on a VPRN site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Right-click on a Routing Instance icon and choose Properties from the contextual menu. The VPRN Site (Edit) form opens with the General tab displayed.

6 Click on the Multicast tab. The MVPN tab is displayed.

7 Configure the MVPN VRF Target Type parameter on the Routing tab:



Note 1 — Route targets are used to identify the VRFs of a VPRN. A PE router that is not a route reflector or an AS border router installs a VPRN route only when its import target matches the target of the route.

Note 2 — A fully-meshed VPRN requires one target for all participating VRFs. A hub-and-spoke VPRN requires VRF import and export targets. The export target of the hub VRF must be the same as the import target of the spoke VRFs. The import target of the hub VRF must be the same as the export target of the spoke VRF. VPRN VRF targets must not overlap.

a If you do not need to specify a VRF target for the site, set the MVPN VRF Target Type parameter to None. Go to step 11.

b If you need to specify a default VRF target for the site, set the MVPN VRF Target Type. Go to step 8.

c If you need to specify import and export VRF targets for the service site, set the MVPN VRF Target Type parameter to Define Import and Export. Go to step 9.

8 Configure the Target Format parameter by performing one of the following steps:

a Specify a two-byte AS number for the default target, if required:

i Configure the parameters:

- Target AS Value
- Target Extended Community Value

The Target AS Value is the Autonomous System number of the PE node. For the Target Extended Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 18.

b To specify an IP Address for the default target, if required:

i Configure the parameters:

- Target IP Address
- Target Community Value

ii Go to step 17.

c Specify a four-byte AS number for the default target, if required:

i Configure the parameters:

- Target AS Value (4Byte)
- Target Community Value

The Target AS Value (4Byte) is the Autonomous System number of the PE node. For the Target Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 17.

9 Configure the Import Target Format parameter by performing one of the following steps:

a Choose None to specify no VRF import target format for the site, then go to step 10.

b Choose AS as the two-byte import target format for the site.

i Configure the parameters:

- Import Target AS Value
- Import Target Extended Community Value

The Import Target AS Value is the two-byte Autonomous System number of the PE node. For the Import Target Extended Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 10.

c Choose IP Address as the import target format for the site.

i Configure the parameters:

- Import Target IP Address
- Import Target Community Value

ii Go to step 10.

d Choose AS-4Byte as the four-byte import target format for the site.

i Configure the parameters:

- Import Target AS Value (4Byte)
- Import Target Community Value

The Import Target AS Value (4Byte) is the four-byte Autonomous System number of the PE node. For the Import Target Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 10.

10 Configure the Export Target Format parameter by performing one of the following steps:

a Choose None to specify no VRF export target format for the site, then go to step 11.

b Choose AS as the two-byte export target format for the site.

i Configure the parameters:

- Export Target AS Value
- Export Target Extended Community Value

The Export Target AS Value parameter is the two-byte Autonomous System number of the PE node. For the Export Target Extended Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 11.

c Choose IP Address as the export target format for the site.

i Configure the parameters:

- Export Target IP Address
- Export Target Community Value

ii Go to step 11.

d Choose AS-4Byte as the four-byte export target format for the site.

i Configure the parameters:

- Export Target AS Value (4Byte)
- Export Target Community Value

The Export Target AS Value (4Byte) parameter is the four-byte Autonomous System number of the PE node. For the Export Target Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 11.

11 Click on the Import Policies tab.

12 Configure the Import Unicast parameter. If you set the parameter to True, go to step 14.

13 Specify the required Unicast import policies by using the Select button to choose a policy from the filtered list.

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5
- Policy 6
- Policy 7
- Policy 8
- Policy 9
- Policy 10
- Policy 11
- Policy 12
- Policy 13
- Policy 14
- Policy 15

14 Click on the Export Policies tab.

15 Configure the Export Unicast parameter. If you set the parameter to True, go to step 18.

16 Specify the required VRF export policies by using the Select button to choose a policy from the filtered list.

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5
- Policy 6
- Policy 7
- Policy 8
- Policy 9
- Policy 10
- Policy 11
- Policy 12
- Policy 13
- Policy 14
- Policy 15

17 Click on the OK button to close the VPRN Site (Edit) form.

18 Close the VPRN Service (Edit) form.

19 Close the Manage Services form.

Procedure 71-6 To enable routing protocols on a VPRN site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Right-click on a Routing Instance icon and choose Properties from the contextual menu. The VPRN Site (Edit) form opens with the General tab displayed.

6 Click on the Routing tab. The Protocols tab is displayed.

7 Configure the parameters on the Protocols tab:

- BGP Enabled
- OSPFv2 Enabled
- OSPFv3 Enabled
- RIP Enabled
- MPLS-TP Enabled
- L2TP Enabled
- WPP Enabled

When you choose a protocol, the site and the protocols that are enabled on the site appear in the list panel.



Note — If both the OSPFv2 Enabled parameter and the OSPFv3 Enabled parameter are disabled, navigate to the Components view of the VPRN, right-click on Protocols, then select Create OSPF Site. The OSPF Site (Create) form opens with the General tab displayed. In the OSPF Instance panel, configure the Version parameter.

8 Click on the Multicast tab to configure multicast for the site, if required.

9 Configure the parameters:

- PIM Enabled
- IGMP Enabled

When you choose a protocol, the site and the protocols that are enabled on the site appear in the list panel.

10 Click on the OK button to close the VPRN Site (Edit) form.

11 Close the VPRN Service (Edit) form.

12 Close the Manage Services form.

Procedure 71-7 To resync soft GRE tunnels on a VPRN site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Right-click on a Routing Instance icon and choose Properties from the contextual menu. The VPRN Site (Edit) form opens with the General tab displayed.

6 Click on the Soft GRE Tunnels tab.

7 Click on the Resync Soft GRE Tunnels button.

8 Close the VPRN Site (Edit) form.

9 Close the VPRN Service (Edit) form.

10 Close the Manage Services form.

Procedure 71-8 To configure a BGP confederation on a VPRN site

Perform this procedure to configure a BGP confederation on a VPRN site. A BGP confederation allows for the full distribution of external routing information within an AS.



Note 1 — You cannot configure BGP confederations when:

- VRF import or export policies are configured on the VPRN site
- a VRF target is configured on the VPRN site
- VPRN GRT lookup or export policies are configured on the VPRN site

Note 2 — You cannot configure VRF import or export policies, VRF target, or GRT lookup or export policies when a BGP confederation is configured.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Right-click on a Routing Instance icon and choose Properties from the contextual menu. The VPRN Site (Edit) form opens with the General tab displayed.

6 Click on the Routing tab. The General tab is displayed.

7 Configure the Confederation Autonomous System parameter. When you set the Confederation Autonomous System to a value other than 0, the BGP Confederations tab appears.

8 Click on the BGP Confederations tab.

9 Click on the Create button. The Confederation (Create) form opens with the General tab displayed.

10 Click on the Members tab.

11 Click on the Create button. The Confederation Member (Create) form opens.

12 Configure the Member AS parameter.

13 Click on the OK button. The Confederation Member (Create) form closes and a dialog box appears.

14 Click on the OK button.

15 Repeat steps 11 to 14 to create additional confederation members.

16 Click on the OK button. The Confederation (Create) form closes and a dialog box appears.

17 Click on the OK button.

18 Click on the OK button to close the VPRN Site (Edit) form.

19 Close the VPRN Service (Edit) form.

20 Close the Manage Services form.

Procedure 71-9 To configure a routing instance on a VPRN site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Right-click on a Routing Instance icon and choose Properties from the contextual menu. The VPRN Site (Edit) form opens with the General tab displayed.

6 Click on the Routing tab. The General tab is displayed.

7 Configure the parameters:

- Router ID
- Maximum Number Of Equal Cost Routes
- Autonomous System
- FIB Priority
- Route Distinguisher Type
- Confederation Autonomous System
- Type
- Ignore NH Metric
- Label Mode
- Carrier Carrier VPN



Note 1 — You cannot configure the Carrier Carrier VPN parameter on a VPRN site if interfaces are configured on the site.

Note 2 — When you set the Route Distinguisher Type parameter to Type 0, the following configurable parameters appear:

- Type 0 Administrative Value
- Type 0 Assigned Value

You can click on the Suggest Value button to let the 5620 SAM assign these values. Choose Generate Unique RD from the drop-down menu.

The Type 0 Administrative Value parameter is the Autonomous System (AS) number of the PE node. For the Type 0 Assigned Value parameter, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

Note 3 — When you set the Route Distinguisher Type parameter to Type 1, the following configurable parameters appear:

- Type 1 IP Address
- Type 1 Assigned Value

When you set the Route Distinguisher Type parameter to Type 2, the following configurable parameters appear:

- Type 2 Administrative Value
- Type 2 Assigned Value

8 Configure the parameters in the GRT panel:

- Enable GRT Lookup
- Allow Local Management

9 Configure the Enforce Maximum Number Of Routes parameter in the Maximum Number Of Routes panel.



Note — When you select the Enforce Maximum Number Of Routes parameter, the following parameters appear:

- Maximum Number Of Routes
- Log Only
- Threshold (%)

10 Configure the Enforce Maximum Number Of IPv6 Routes parameter in the Maximum Number Of IPv6 Routes panel.



Note — When you select the Enforce Maximum Number Of IPv6 Routes parameter, the following parameters appear:

- Maximum Number Of IPv6 Routes
- Log Only
- Threshold (%)

11 Configure the parameters:

- Single SFM Overload Admin State
- Hold-Off Time (seconds)

The Hold-Off Time (seconds) parameter and read-only attributes Overload State, Overload Start, and Overload Duration are only displayed when the Single SFM Overload Admin State parameter is set to Up.

12 Configure the Enforce Maximum Number Of Multicast Routes parameter in the Maximum Number Of Multicast Routes panel.



Note — When you enable the Enforce Maximum Number Of Multicast Routes parameter, the following configurable parameters appear:

- Maximum Number Of Multicast Routes
- Log Only
- Threshold (%)

13 Click on the VRF Target to configure a VRF instance.

14 Configure the VRF Target Type parameter:



Note 1 — Route targets are used to identify the VRFs of a VPRN. A PE router that is not a route reflector or an AS border router installs a VPRN route only when its import target matches the target of the route.

Note 2 — A fully-meshed VPRN requires one target for all participating VRFs. A hub-and-spoke VPRN requires VRF import and export targets. The export target of the hub VRF must be the same as the import target of the spoke VRFs. The import target of the hub VRF must be the same as the export target of the spoke VRF. VPRN VRF targets must not overlap.

a Specify None if you do not need to specify a VRF target for the site. Go to step 18.

b Specify Define Default if you need to specify a default VRF target for the site. Go to step 15.

c Specify Define Import and Export if you need to specify import and export VRF targets for the service site. Go to step 16.

15 Configure the Target Format parameter by performing one of the following steps:

a To specify a two-byte AS number for the default target, if required:

i Configure the parameters:

- Target AS Value
- Target Extended Community Value

You can click on the Suggest Value button to let the 5620 SAM assign these values. Choose Generate Unique VRF Target from the drop-down menu.

The Target AS Value parameter is the Autonomous System number of the PE node. For the Target Extended Community Value parameter, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 18.

b To specify an IP Address for the default target, if required:

i Configure the parameters:

- Target IP Address
- Target Community Value

ii Go to step 18.

c To specify a four-byte AS number for the default target, if required:

i Configure the parameters:

- Target AS Value (4Byte)
- Target Community Value

You can click on the Suggest Value button to let the 5620 SAM assign these values. Choose Generate Unique VRF Target from the drop-down menu.

The Target AS Value (4Byte) is the Autonomous System number of the PE node. For the Target Community Value parameter, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 18.

16 Configure the Import Target Format parameter by performing one of the following steps:

a Choose None to specify no VRF import target format for the site, then go to step 17.

b Choose AS as the two-byte import target format for the site.

i Configure the parameters:

- Import Target AS Value
- Import Target Extended Community Value

You can click on the Suggest Value button to let the 5620 SAM assign these values. Choose Generate Unique VRF Target from the drop-down menu.

The Import Target AS Value parameter is the two-byte Autonomous System number of the PE node. For the Import Target Extended Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 17.

c Choose IP Address as the import target format for the site.

i Configure the parameters:

- Import Target IP Address
- Import Target Community Value

ii Go to step 17.

d Choose AS-4Byte as the four-byte import target format for the site.

i Configure the parameters:

- Import Target AS Value (4Byte)
- Import Target Community Value

You can click on the Suggest Value button to let the 5620 SAM assign these values. Choose Generate Unique VRF Target from the drop-down menu.

The Import Target AS Value (4Byte) is the four-byte Autonomous System number of the PE node. For the Import Target Community Value parameter, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 17.

17 Configure the Export Target Format parameter by performing one of the following steps:

a Choose None to specify no VRF export target format for the site, then go to step 18.

b Choose AS as the two-byte export target format for the site.

i Configure the parameters:

- Export Target AS Value
- Export Target Extended Community Value

The Export Target AS Value parameter is the two-byte Autonomous System number of the PE node. For the Export Target Community Value parameter, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 18.

c Choose IP Address as the export target format for the site.

i Configure the parameters:

- Export Target IP Address
- Export Target Community Value

ii Go to step 18.

d Choose AS-4Byte as the four-byte export target format for the site.

i Configure the parameters:

- Export Target AS Value (4Byte)
- Export Target Community Value

The Export Target AS Value (4Byte) is the four-byte Autonomous System number of the PE node. For the Export Target Community Value parameter, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 18.

18 Configure ingress multicast forwarding, if required.

i Click on the Mcast Path Mgmt .

ii Click on the Select button beside the Name parameter. The Select Ingress Info Policy - Service L3 Routing list form opens.

iii Choose an ingress info policy and click on the OK button. The Select Ingress Info Policy - Service L3 Routing list form closes.



Note — The Mcast Path Mgmt Channels tab displays data on the operational channels after actual traffic from a specific multicast source for a specific multicast group passes through the virtual router. You must click on the Search button to refresh the data. See chapter 42 for a listing of the displayed operational channel parameters.

19 Click on the OK button to close the VPRN Site (Edit) form.

20 Close the VPRN Service (Edit) form.

21 Close the Manage Services form.

Procedure 71-10 To bind a VPRN site to service tunnels

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Right-click on a Routing Instance icon and choose Properties from the contextual menu. The VPRN Site (Edit) form opens with the General tab displayed.

6 Click on the SDP Binding tab. The Spoke SDP Bindings tab is displayed.

7 Click on the Auto-Bind tab to configure the binding of the site to service tunnels.

8 Configure the Transport parameter.

a Choose None to explicitly specify service tunnels and circuits for the service.

b Choose LDP for the service to be automatically bound to MPLS service tunnels utilizing LDP.



Note — To use MPLS as the transport type, you must bind LSPs to service tunnels during service tunnel configuration. See Procedure 27-1 for more information.

c Choose RSVP-LSP for the service to be automatically bound to MPLS service tunnels utilizing RSVP-LSP.



Note — The RSVP-LSP option is available only on the 7450 ESS in mixed mode, the 7710 SR, 7750 SR, and 7950 XRS.

d Choose RSVP or LDP for the service to be bound to MPLS service tunnels using RSVP or LDP.

This choice provides the ability to simultaneously support both tunnel options, in networks that have a mixture of LDP and RSVP-TE in place. 5620 SAM always tries to resolve the VPN route by using RSVP-LSP tunnels first (lowest metric). If no RSVP-LSP service tunnels are available, then tunnels configured for LDP are used. If RSVP-LSP tunnels subsequently become available again, then the route resolution automatically returns to RSVP-LSP.



Note — The RSVP or LDP option is available only on the a 7450 ESS in mixed mode, and on a 7710 SR, 7750 SR, or 7950 XRS.

e Choose GRE for the service to be automatically bound to GRE service tunnels.

9 Click on the OK button to close the VPRN Site (Edit) form.

10 Close the VPRN Service (Edit) form.

11 Close the Manage Services form.

Procedure 71-11 To configure VRF import and export policies on a VPRN site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Right-click on a Routing Instance icon and choose Properties from the contextual menu. The VPRN Site (Edit) form opens with the General tab displayed.

6 Click on the VRF Import Policies tab.

7 Specify the required VRF import policies by using the Select button to choose a policy from the filtered list form.

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5
- Policy 6
- Policy 7
- Policy 8
- Policy 9
- Policy 10
- Policy 11
- Policy 12
- Policy 13
- Policy 14
- Policy 15

8 Click on the OK button. The filtered list form closes.

9 Click on the VRF Export Policies tab.

10 Specify the required VRF export policies by using the Select button to choose a policy from the filtered list form.

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5
- Policy 6
- Policy 7
- Policy 8
- Policy 9
- Policy 10
- Policy 11
- Policy 12
- Policy 13
- Policy 14
- Policy 15

11 Click on the OK button. The filtered list form closes.

12 Click on the OK button to close the VPRN Site (Edit) form.

13 Close the VPRN Service (Edit) form.

14 Close the Manage Services form.

Procedure 71-12 To configure static routes on a VPRN site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Right-click on a Routing Instance icon and choose Properties from the contextual menu. The VPRN Site (Edit) form opens with the General tab displayed.

6 Click on the Routing tab. The General tab is displayed.

7 Click on the Static Routes tab.

8 Click on the Create button to define a static route that the PE VRF is to exchange with the CE. The Static Route (Create) form opens.

9 Configure the parameters:

- Auto-Assign ID
- Static Route ID
- BFD Enabled
- Forwarding Class Name
- Forwarding Class Priority
- Community
- Description

10 Configure the parameters in the Destination panel:

- Destination
- Multicast Capable Peers
- Prefix Length
- Type
- IP Address

The IP Address parameter is configurable when the Type parameter is set to an option other than Black Hole.

11 Configure the parameters in the Other panel:

- Preference
- Metric
- Administrative State
- Tag

12 Configure the parameters in the CPE Check panel:

- Enable CPE Check
- Target IP Address
- Interval (seconds)
- Drop Count
- Log

The Target IP Address, Interval (seconds), Drop Count, and Log parameters are configurable only when the Enable CPE Check parameter is enabled.

13 Click on the Select button next to the Prefix List Name in the Prefix List panel. The Select...-Static Route list form opens.

14 Choose a prefix list name and click on the OK button. The Select...-Static Route list form closes.



Note — You cannot specify a Prefix List if BFD Enabled or Enable CPE Check parameters are enabled for the static route.

15 Configure the Prefix List Flag parameter. The Prefix List Flag parameter is configurable only when you choose a prefix list.

16 Click on the OK button. The Static Route (Create) form closes and the VPRN Site (Edit) form reappears.

17 Click on the OK button to close the VPRN Site (Edit) form.

18 Close the VPRN Service (Edit) form.

19 Close the Manage Services form.

Procedure 71-13 To configure a GSMP group on a VPRN site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Right-click on a Routing Instance icon and choose Properties from the contextual menu. The VPRN Site (Edit) form opens with the General tab displayed.

6 Click on the GSMP tab.

7 Click on the Create button. The GSMP Group (Create) form opens with the General tab displayed.

8 Configure the following parameters:

- Displayed Name
- Description
- Administrative State
- Keep-Alive (seconds)
- Hold Multiplier
- Enable Idle Filter
- Enable Persistency Database
- OAM Administrative State
- Dynamic Topology Discovery

9 Click on the GSMP Group Neighbor tab.

10 Click on the Create button. The GSMP (Create) form opens with the General tab displayed.

11 Configure the following parameters:

- IP Address
- Description
- Administrative State
- Local Address
- Priority Type
- Priority Precedence
- Priority Dscp

The Priority Dscp parameter is configurable when you set the Priority Type to Dscp.

The Priority Precedence parameter is configurable when you set the Priority Type to Precedence.

12 Click on the OK button. The GSMP (Create) form closes.

13 Click on the OK button. The GSMP Group (Create) form closes.

14 Click on the OK button to close the VPRN Site (Edit) form.

15 Close the VPRN Service (Edit) form.

16 Close the Manage Services form.

Procedure 71-14 To configure a local DHCPv4 server on a VPRN site



Note — To configure a local DHCPv6 server on a VPRN site go to Procedure 71-15.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

4 Expand the Sites icon in the service navigation tree.

5 Right-click on a Routing Instance icon and choose Properties from the contextual menu. The VPRN Site (Edit) form opens with the General tab displayed.

6 Click on the RADIUS/DHCP/Diameter tab. The Local DHCP Servers tab is displayed.

7 Configure a local DHCPv4 server on the routing instance as described in Procedure 22-2, steps 5 to 19.

8 Click on the OK button. The Local DHCP Server (Create) form closes and a dialog box appears.

9 Click on the OK button. The VPRN Site (Edit) form reappears.

10 Click on the OK button to close the VPRN Site (Edit) form.

11 Close the Manage Services form.

Procedure 71-15 To configure a local DHCPv6 server on a VPRN site



Note — To configure a local DHCPv4 server on a VPRN site go to Procedure 71-14.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with General tab displayed.

4 Expand the Sites icon in the service navigation tree.

5 Right-click on a Routing Instance icon and choose Properties from the contextual menu. The VPRN Site (Edit) form opens with the General tab displayed.

6 Click on the RADIUS/DHCP/Diameter tab. The Local DHCP Servers tab is displayed.

7 Configure a local DHCPv6 server on the routing instance as described in Procedure 22-3, steps 5 to 15.

8 Click on the OK button. The Local DHCP Server (Create) form closes and a dialog box appears.

9 Click on the OK button. The VPRN Site (Edit) form reappears.

10 Click on the OK button to close the VPRN Site (Edit) form.

11 Close the Manage Services form.

Procedure 71-16 To configure DSCP on a VPRN site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Right-click on a Routing Instance icon and choose Properties from the contextual menu. The VPRN Site (Edit) form opens with the General tab displayed.

6 Click on the Self Generated Traffic tab. The DSCP Marking tab is displayed with a list of all the applications for which the DSCP can be set.

- **i** Choose an application to view or edit the DSCP setting.
- **ii** Click on the Properties button. An Application DSCP Marking form opens.
- **iii** Configure the DSCP parameter.
- **iv** Click on the Apply button. A dialog box appears. Click on the OK button.
- **v** Click on the DSCP Mapping tab. A list of DSCP types and corresponding forwarding classes is displayed.
- **vi** Choose a DSCP to view or edit the forwarding class.
- **vii** Click on the Properties button. An Application DCSP Marking form opens.
- **viii** Configure the Forwarding Class parameter.
- **ix** Click on the Apply button. A dialog box appears. Click on the OK button.
- **x** Click on the Dot1p Marking tab. A list of applications for which the dot1p can be set is displayed.

xi Choose a dot1p to view or edit the setting and then click on the Properties button. An Application Dot1p Marking form opens.

xii Configure the dot1p parameter.

xiii Click on the OK button. A dialog box appears. Click on the OK button.

7 Click on the OK button to close the VPRN Site (Edit) form.

8 Close the VPRN Service (Edit) form.

9 Close the Manage Services form.

Procedure 71-17 To configure an override source IP address or L3 interface on a VPRN site

Perform the following procedure to configure an override source IP address or L3 interface for use by a selected IP application, if required.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Right-click on a Routing Instance icon and choose Properties from the contextual menu. The VPRN Site (Edit) form opens with the General tab displayed.

6 Click on the Source Addresses tab.

7 Click on the Create button. The Source Address (Create) form opens.

8 Configure the Source IP Application parameter.

9 Specify the source address for the IP application server by performing one of the following:



Note — If you choose the interface index option, the router used for this VPRN must already have an access interface created for its routing instance.

a Specify the source IP address of the IP application server:

i Set the Source Address Termination parameter to IP Address.

ii Configure the Source IP Address parameter. Enter a valid IP address that the VPRN virtual routing instance will identify.

iii Go to step 10.



Note 1 — An IPv6 address option for the Source IP Address parameter is available when the IPv6 Allowed parameter is set during network interface creation. See chapter 22 for more information about creating a network interface.

Note 2 — You must select an IPv6 Source IP Address before you can select IPv6 Source IP Applications.

b Specify the primary address of the L3 network interface as the source address of the IP application server:

i Set the Source Address Termination parameter to Interface Index.

ii Click on the Select button to choose an interface. The Select Source Address VPRN Interface - Source Address form opens.

iii Choose an interface and click on the OK button. The IP address and Interface ID of the L3 interface appear on the form.

10 Click on the OK button. The Source Address (Create) form closes and the VPRN Site (Edit) form reappears. The IP application source address and parameters appear on the form.

11 Click on the OK button to close the VPRN Site (Edit) form.

12 Close the VPRN Service (Edit) form.

13 Close the Manage Services form.

Procedure 71-18 To configure IGMP host tracking on a VPRN site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Right-click on a Routing Instance icon and choose Properties from the contextual menu. The VPRN Site (Edit) form opens with the General tab displayed.

6 Click on the IGMP Host Tracking tab.

7 Configure the parameters:

- Expiry Time (seconds)
- Administrative State

8 Click on the OK button to close the VPRN Site (Edit) form.

9 Close the VPRN Service (Edit) form.

10 Close the Manage Services form.

Procedure 71-19 To configure WLAN gateway functionality on a VPRN site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Right-click on a Routing Instance icon and choose Properties from the contextual menu. The VPRN Site (Edit) form opens with the General tab displayed.

6 Click on the General tab and configure the Enable WLAN GW parameter.

7 Click on the WLAN GW tab. The General tab is displayed.

8 Configure the APN Network Identifier parameter.

9 Click on the Mobile GW Address Map tab, and click on the Create button. The Mobile Gateway Address Map (Create) form opens.

10 Configure the Mobile Gateway Address Prefix and Prefix Length parameters.

11 Click on the Select button beside the Mobile Gateway Profile field to specify a mobile gateway profile policy.

12 Click on the OK button. The Mobile Gateway Address Map (Create) form closes.

13 Click on the OK button to close the VPRN Site (Edit) form.

14 Close the VPRN Service (Edit) form.

15 Close the Manage Services form.

Procedure 71-20 To configure DNS for a VPRN site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Right-click on a Routing Instance icon and choose Properties from the contextual menu. The VPRN Site (Edit) form opens with the General tab displayed.

6 Configure the Enable DNS parameter.

7 Click on the DNS tab and configure the parameters:

- Administrative State
- Primary Address
- Secondary Address
- Tertiary Address
- IPv4 Source Address
- IPv6 Source Address

8 Click on the OK button to close the VPRN Site (Edit) form.

9 Close the VPRN Service (Edit) form.

10 Close the Manage Services form.

Procedure 71-21 To configure route aggregates on a VPRN site

Route aggregation allows you to group a number of routes with common IP prefixes into a single entry in the routing table. This reduces the number of routes that need to be advertised by the hosting router and reduces the number of routes in the routing tables of downstream routers.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Right-click on a Routing Instance icon and choose Properties from the contextual menu. The VPRN Site (Edit) form opens with the General tab displayed.

6 Click on the Routing tab. The General tab is displayed.

7 Click on the Route Aggregation tab.



Note — Route aggregation for VPRN sites is supported on 7450 ESS in mixed mode, 7750 SR, 7710 SR, and 7950 XRS nodes.

8 Click on the Create button. The Aggregation (Create) form opens.

9 Configure the parameters:

- IP Address Prefix
- Mask
- Summary Only
- As Set
- Aggregator
- Next Hop Type
- Community
- Aggregator AS
- Aggregator IP Address
- Indirect Address

The IP Address Prefix you enter must be an IPv4 address in the form x.x.x.0, where the last integer is the host bits and must have a value of 0.

The Next Hop Type parameter is configurable only on a Release 10.0 R4 or later 7450 ESS, 7710 SR, or 7750 SR.

The Aggregator AS and Aggregator IP Address parameters are configurable when the Aggregator parameter value is set to True. The Indirect Address parameter is configurable when the Next Hop Type parameter is set to Indirect.

10 Click on the OK button to close the VPRN Site (Edit) form.

11 Close the VPRN Service (Edit) form.

12 Close the Manage Services form.

Procedure 71-22 To configure an L3 access interface on a VPRN site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service.

4 Click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

5 On the navigation tree, expand the Sites icon and the site on which you need to configure the access interface. For information about how to add a GNE service interface to a VPRN service, see Procedure 71-49.

6 Perform one of the following.

a Create an L3 access interface on the site:

i Right-click on Access Interfaces and choose Create L3 Access Interface. The VPRN L3 Access Interface (Create) form opens with the General tab displayed.

ii Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Admin Link Local Address
- Admin Link Local Address Preferred

The Admin Link Local Address and Admin Link Local Address Preferred parameters are only configurable when the IPv6 Allowed parameter is enabled.

b Configure an existing VPRN L3 access interface:

i Expand the Sites icon in the service navigation tree.

ii Expand the Routing Instance icon.

iii Expand the L3 Access Interfaces icon, right-click on the L3 access interface you need to configure and choose Properties from the contextual menu. The VPRN L3 Access Interfaces (Edit) form opens with the General tab displayed.

7 Configure the parameters:

- Description
- Administrative State
- MAC Address
- Allow Directed Broadcasts
- Loopback Enabled
- Cflowd Type
- Trusted
- Class
- IPv6 Allowed
- Enable Ingress FlowSpec IPv4
- Enable Ingress FlowSpec IPv6
- QoS Route Lookup IPv4
- QoS Route Lookup IPv6
- Calling Station ID
- Enable Ingress Stats
- Enable MAC Accounting Stats
- Configured IP MTU (Octets)
- URPF Check State IPv4
- URPF Check Mode IPv4
- URPF Check State IPv6
- URPF Check Mode IPv6
- Unnumbered Type
- IP Address
- Interface Name
- Tunnel Fault Notification

The Enable Ingress FlowSpec IPv4 and Enable Ingress FlowSpec IPv6 parameters appear only if a port is assigned to the L3 access interface.

The Unnumbered Type parameter is configurable when the Class parameter is set to Unnumbered.

The IP Address parameter is configurable when the Unnumbered Type parameter is set to IP Address.

The Interface Name parameter is configurable when the Unnumbered Type parameter is set to Name.

The URPF Check State IPv6 and URPF Check Mode IPv6 parameters are only configurable when the IPv6 Allowed parameter is enabled.

The Tunnel Fault Notification parameter is configurable on interfaces where the device has ports configured in access or hybrid mode with QinQ encapsulation.

If you are configuring a tunnel facility MEP, Tunnel Fault Notification must be set to Accept, in order to receive the fault notification from the tunnel facility MEP.

8 If the Loopback Enabled parameter in step 7 is enabled, you cannot associate a port with the L3 access interface. Go to step 18.

9 Bind an application profile to the VPRN L3 access interface, if required:

i Click on the Select button beside the Application Profile parameter in the Application Assurance panel. The Application Profile String: - VPRN L3 Access Interface list form opens.

ii Choose a profile and click on the OK button. The Application Profile String - VPRN L3 Access Interface list form closes and the L3 Access Interface (Create) form is refreshed with the Application Profile information.



Note — The Application Profile String: - VPRN L3 Access Interface list form only displays local profiles that already exist on the NE.

10 Choose one of the following AA transit policy types, if required.



Note 1 — You can only associate one AA transit policy type with a service object.

Note 2 — To bind a transit policy to an L3 access interface, a port must already exist on the interface.

Note 3 — You can bind a transit policy to only one L3 access interface or spoke SDP binding per NE.

Note 4 — The transit policy and the application profile must belong to the same application assurance group or partition.

a Associate an AA transit IP policy with the service object:

i Click on the Select button in the Transit IP Policy panel. The Select Transit IP Policy form opens.

ii Choose a transit IP policy and click on the OK button.

b Associate an AA transit prefix policy with the service object:

i Click on the Select button in the Transit Prefix Policy panel. The Select Transit Prefix Policy form opens.

ii Choose a transit IP policy and click on the OK button.

11 Associate a host lockout policy with the L3 access interface, if required. Click on the Select button in the Host Lockout panel to select a policy.

12 Click on the Port tab.

13 Click on the Select button to choose a port for the L3 access interface. The Select Terminating Port - VPRN L3 Access Interface form opens.



Note 1 — The form lists only ports in access or hybrid mode, or PW ports. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. The port is then listed when you click on the Search button.

Note 2 — The form only lists PW ports that are bound to a service tunnel. See Procedure 27-1 for information about creating a service tunnel with a PW port binding.

14 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - VPRN L3 Access Interface form closes, and the VPRN L3 Access Interface (Create) form displays the port information.

Once the port is selected, a number of other tabs are also displayed on the form.

15 Configure the parameters:

- Auto-Assign ID
- Outer Encapsulation Value
- Inner Encapsulation Value
- Outer Encapsulation Value (VPI)
- Inner Encapsulation Value (VCI)
- SAP Description
- SAP Administrative State

The Auto-Assign ID parameter is configurable if the port uses dot1q encapsulation. When the parameter is enabled, the 5620 SAM automatically configures the Outer Encapsulation Value parameter using the lowest unassigned value.



Note — You can set the Auto-Assign ID parameter to be the default parameter for dot1q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter on the User Preferences form. Choose Application→ User Preferences from the main menu.

The Inner Encapsulation Value is configurable only when the port is an Ethernet or frame relay port with QinQ encapsulation.

The Outer Encapsulation Value (VPI) and Inner Encapsulation Value (VCI) parameters are configurable only for ATM ports.

16 If the selected port uses FR encapsulation, configure Frame Relay for the interface. Otherwise, go to step 17.

i Click on the Frame Relay tab.

ii Set the FRF-12 Mode parameter to Enabled.

iii Configure the parameters:

- FRF-12 End-To-End Fragment Threshold
- Scheduling Class
- Fragment Interleave



Note — If a bundle is selected in step 14, only the Scheduling Class parameter is configurable.

17 The ATM tab is configurable when the interface port is an ATM port. Specify OAM functionality and assign ingress and egress ATM policies to the interface, if required. Otherwise, go to step 18.

i Click on the ATM tab.

ii Configure the parameters:

- AAL5 Encapsulation
- ATM OAM Alarm Cell Handling
- Periodic ATM OAM Loopback

iii Click on the Select button in the Ingress ATM Policy panel to choose an ingress ATM policy. The Select Ingress ATM Policy - ATM Configuration form opens.

iv Choose an ingress ATM policy and click on the OK button. The Select Ingress ATM Policy - ATM Configuration form closes and the L3 Access Interface form reappears with the ingress ATM policy information displayed.

v Click on the Select button in the Egress ATM Policy panel to choose an egress ATM policy. The Select Egress ATM Policy - ATM Configuration form opens.

vi Choose an egress ATM policy and click on the OK button. The Select Egress ATM Policy - ATM Configuration form closes and the L3 Access Interface (Edit) form reappears with the egress ATM policy information displayed.

18 Click on the OK button. The VPRN L3 Access Interface (Create) form closes, and the VPRN Site (Edit) form reappears with the new interface information displayed in the service navigation tree.

Repeat steps 6 to 18 to create another L3 access interface for the site in the VPRN service.

Procedure 71-23 To configure NTP on a VPRN site



Note — NTP must be enabled on the base router before it can be configured on a VPRN site. See Procedure 15-10 for information about configuring NTP on the 7705 SAR, 7750 MG, and 7750 SR.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree. A list of service sites appears.

5 Choose a site from the list. The properties of the site are displayed in the right panel.

6 In the General tab, set the value of the NTP State parameter to Enabled.

7 Click on the NTP tab.

8 Configure the parameters:

- Authentication Check
- Admin State
- Server Authenticate

9 As required, create an authentication key by performing the following:

i Click on the Authentication tab.

ii Click on the Create button. The Network Time Protocol Authentication (New Instance) form opens.

iii Configure the parameters:

- Authentication Key ID
- Authentication Key
- Authentication Key Type

iv Click on the OK button. The new authentication key appears in the list.

10 As required, configure an NTP broadcast source by performing the following:

i Click on the Broadcast tab.

ii Click on the Create button. The NTP Broadcast (New Instance) form opens.

iii Click on the Select button. The Select Source Interface (NTP Broadcast) form opens.

iv Configure the filters, and click on the Search button. A list of available source interfaces appears.

v Select a source interface and click on the OK button.

vi Configure the parameters:

- Direction
- Authentication Key ID
- NTP Version
- Time To Live

vii Click on the OK button. The new source interface appears in the list.

11 Click on the OK button. The VPRN Service (Edit) form closes.

Procedure 71-24 To configure custom object attributes for AA reporting to the 5670 RAM on a VPRN L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Routing Instance icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The VPRN L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the 5670 RAM Parameters tab.

8 Click on the Reporting tab.

9 Click on the Create button. The AA Reporting (Create) form opens.

10 Configure the parameters:

- Customer Name
- Subscriber Name
- Subscriber Class
- Subscriber Type
- Total Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 1 Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 2 Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 3 Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 4 Bandwidth Upstream (Kbps)
- Downstream (Kbps)

11 Click on the OK button. The AA Reporting (Create) form closes and the reporting object is displayed in the list.

12 Close the VPRN L3 Access Interface (Edit) form.

13 Click on the OK button to close the VPRN Site (Edit) form.

14 Close the VPRN Service (Edit) form.

15 Close the Manage Services form.

Procedure 71-25 To assign ingress and egress QoS policies to a VPRN L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Routing Instance icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The VPRN L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the QoS tab.



Note — The QoS tab is configurable only if a port is assigned to the interface.

8 Configure the Ingress Match QinQ Dot1P parameter.

The Ingress Match QinQ Dot1P parameter is configurable only when the encapsulation type of the port is BCP dot1q, dot1q, or QinQ.

9 Click on the Select button in the Ingress Policy panel to choose an ingress QoS policy. The Select Ingress Policy - L3 Access Interface form opens.

10 Use the configurable filter and Search button to choose a policy, and click on the OK button. The Select Ingress Policy - L3 Access Interface form closes and the L3 Access Interface (Edit) form reappears with the ingress QoS policy information displayed.



Note — If you select an ingress policy which has a forwarding class mapped to an ingress queue group, you must ensure that the port you selected in step 14 of Procedure 71-22 has the access ingress queue group with the same name created on it.

See Procedure 16-1 for more information about how to configure Ethernet ports. See chapter 42 for more information about queue group template policies.

11 Click on the Ingress Queue Group Template Policy Select button in the Forwarding Plane Redirect panel to choose a policy. The Select Forwarding Plane Queue Group Instance form opens.

12 Choose a policy and click on the OK button. The Select Forwarding Plane Queue Group Instance form closes. The VPRN L3 Access Interface (Create) form refreshes with the Ingress Queue Group Template Policy information displayed.

13 Configure the Instance ID parameter.

14 Configure the Egress Mark QinQ Top Bits Only parameter.

The Egress Mark QinQ Top Bits Only parameter is configurable only when the encapsulation type of the port is BCP dot1q, dot1q, or QinQ.

15 Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - L3 Access Interface form opens.

16 Use the configurable filter and Search button to choose a QoS policy, and click on the OK button. The Select Egress Policy - L3 Access Interface form closes and the L3 Access Interface (Edit) form refreshes with the egress QoS policy information displayed.



Note 1 — If you select an egress policy which has a forwarding class mapped to an egress queue group, you must ensure that the port you selected in step 14 of Procedure 71-22 has the access egress queue group with the same name created on it.

See Procedure 16-1 for more information about how to configure Ethernet ports. See chapter 42 for more information about queue group template policies.

Note 2 — Queue Group Template policies are not applicable to L3 interfaces associated with HSMDA ports.

17 Click on the Select button in the Port Redirect panel to choose an Egress Queue Group Template Policy, if required. The Select Egress Queue Group Template Policy form opens.



Note — Selecting an Egress Queue Group Template Policy here permits the redirection of Ethernet traffic packets to a queue ID specified in the SAP's egress port queue group. The following properties and restrictions apply:

- If an Egress Queue Group Template Policy is specified here, the policy must have port redirection enabled.
- You cannot use policy-based redirection with the queue group when the SAP has SAP-based redirection enabled.
- Port access egress redirection is only supported on Ethernet/LAG ports. It is not supported on SAPs bound on non-Ethernet, Eth-tunnel, or CCAG ports.
- Supported ports include access, hybrid, and HSMDA.
- Queue groups can be applied to SAPs that incorporate LAGs. The LAGs can include port members from just a single card or from multiple cards.
- If you edit a LAG incorporated by the SAP, you cannot remove the last LAG member if a queue group reference exists to the containing SAP.
- You cannot add a secondary LAG member that has a queue group mismatch with primary LAG member.

18 Choose an Egress Queue Group Template Policy and click on the OK button. The Select Egress Queue Group Template Policy form closes, and the L3 Access Interface (Create) form refreshes with the Egress Queue Group Template Policy information displayed.

19 If you are configuring an L3 access interface for a 7710 SR or 7705 SAR, or if the port you selected in step 14 of Procedure 71-22 is not an HSMDA port, then go to step 26.

20 Configure the Packet Byte Offset (bytes) parameter, if required. You must enable the associated Override check box if you need to configure this parameter.

21 Click on the Select button in the Egress HSMDA Override panel to choose a WRR policy. The Select WRR Policy form opens.

22 Choose a WRR policy and click on the OK button. The Select WRR Policy form closes and the VPRN L3 Access Interface (Edit) form reappears with the WRR policy information displayed.

23 Click on the Select button in the Egress HSMDA Override panel to choose an HSMDA egress secondary shaper policy. The Select Secondary Shaper form opens.

24 Choose a secondary shaper and click on the OK button. The Select Secondary Shaper form closes and the VPLS L2 Access Interface (Create) form reappears with the secondary shaper information displayed.

25 Configure the parameters:

- Use Shared Queue
- Use Multipoint Shared Queue

26 Close the VPRN L3 Access Interface (Edit) form.

27 Click on the OK button to close the VPRN Site (Edit) form.

28 Close the VPRN Service (Edit) form.

29 Close the Manage Services form.

Procedure 71-26 To configure scheduling on a VPRN L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Routing Instance icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The VPRN L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Schedulers tab.

Note — The Schedulers tab is configurable only if a port is assigned to the SAP in Procedure 71-22.

8 To configure scheduling on a 7705 SAR site, perform the following steps. Otherwise, go to step 9.

Note 1 — For the 7705 SAR, scheduler behavior is determined by the scheduler mode, which is 4-Priority by default. You can only configure the Egress and Ingress Aggregate Rate Limit parameters when the Scheduler Mode parameter is set to 16-Priority. You can set the Scheduler Mode to 16-Priority only when the port is on an MDA that supports 16-Priority. See the 7705 SAR documentation for more information.

Note 2 — If you change the Scheduler Mode parameter from 16-Priority to 4-Priority, the 5620 SAM automatically restores the default settings for the Egress Aggregate Rate Limit and Ingress Aggregate Rate Limit panels when you click on the Apply or OK button.

i In the Egress Scheduler panel, configure the Scheduler Mode parameter.

ii In the Ingress Scheduler panel, configure the Scheduler Mode parameter.

iii If you set the Scheduler Mode parameter to 16-Priority in the Egress Scheduler panel or Ingress Scheduler panel, configure the parameters in the Egress Aggregate Rate Limit panel and Ingress Aggregate Rate Limit panel, as required. Otherwise, go to step 11.

- Assign Aggregate Rate Limit
- Aggregate Rate Limit (kbps)
- Assign Aggregate CIR
- Aggregate CIR (kbps)

iv Go to step 11.

9 Specify that an aggregation scheduler policy is not applied to the interface. Otherwise, go to step 10.

i Set the Aggregation parameter to off.

Note — The Aggregation parameter is not configurable if the port you selected in step 14 of Procedure 71-22 is an HSMDA port.

ii Configure the parameters:

- Aggregate Rate Limit (kbps)
- Frame-Based Accounting



Note 1 — The Aggregate Rate Limit (kbps) and Frame-Based Accounting parameters are configurable only when there is no scheduler specified in the Egress Scheduler panel.

Note 2 — The Frame-Based Accounting parameter is not configurable if the port you selected in step 14 of Procedure 71-22 is an HSMDA port.

Note 3 — You cannot specify an egress scheduler when the Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

iii Click on the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - VPRN L3 Access Interface form opens.

iv Choose an ingress scheduler and click on the OK button. The Select Ingress Scheduler - L3 Access Interface form closes, and the VPRN L3 Access Interface (Create) form refreshes with the ingress scheduler information displayed.

v Click on the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Policer Control Policy form opens.

vi Choose a policer control policy and click on the OK button. The Select Policer Control Policy form closes and the VPRN L3 Access Interface (Edit) form reappears with the ingress policer control policy information displayed.

vii If the port you selected in step 14 of Procedure 71-22 is an HSMDA port, go to step 11.

viii Click on the Select button in the Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - L3 Access Interface form opens.

ix Choose an egress scheduler and click on the OK button. The Select Egress Scheduler - L3 Access Interface form closes, and the L3 Access Interface (Create) form refreshes with the egress scheduler information displayed.

x Click on the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Policer Control Policy form opens.

xi Choose a policer control policy and click on the OK button. The Select Policer Control Policy form closes and the VPRN L3 Access Interface (Edit) form reappears with the egress policer control policy information displayed.

xii Go to step 11.

10 Specify that an aggregation scheduler policy is applied to the interface.



Note — You cannot specify an access scheduler policy if the port you selected in step 14 of Procedure 71-22 is an HSMDA port. Go to step 11.

i Set the Aggregation parameter to on.

ii Click on the Select button in the Aggregation Scheduler panel to choose an aggregation scheduler. The Select Aggregation Scheduler - L3 Access Interface form opens.

iii Choose an aggregation scheduler and click on the OK button. The Select Aggregation Scheduler - L3 Access Interface form closes, and the L3 Access Interface (Create) form refreshes with the aggregation scheduler information displayed.

11 Close the VPRN L3 Access Interface (Edit) form.

12 Click on the OK button to close the VPRN Site (Edit) form.

13 Close the VPRN Service (Edit) form.

14 Close the Manage Services form.

Procedure 71-27 To assign ingress and egress ACL filters to a VPRN L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Routing Instance icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The VPRN L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the ACL tab.

8 Click on the Select button in the Ingress Filter panel to choose an ingress IPv4 ACL filter. The Select Ingress Filter - L3 Access Interface form opens.

9 Choose an ingress ACL filter and click on the OK button. The Select Ingress Filter - L3 Access Interface form closes and the L3 Access Interface (Edit) form reappears with the ingress IPv4 ACL filter information displayed.

10 Click on the Select button in the Egress Filter panel to choose an egress IPv4 ACL filter. The Select Egress Filter - L3 Access Interface form opens.

11 Choose an egress ACL filter and click on the OK button. The Select Egress Filter - L3 Access Interface form closes and the L3 Access Interface (Edit) form reappears with the egress IPv4 ACL filter information displayed.

12 If the L3 Access Interface supports IPv6 addressing, perform the following steps. Otherwise, go to step 17.

13 Click on the Select button in the IPv6 Ingress Filter panel to choose an ingress IPv6 ACL filter. The Select IPv6 Ingress Filter - L3 Access Interface form opens.

14 Choose an ingress ACL filter and click on the OK button. The Select IPv6 Ingress Filter - L3 Access Interface form closes and the L3 Access Interface (Edit) form reappears with the ingress IPv6 ACL filter information displayed.

15 Click on the Select button in the IPv6 Egress Filter panel to choose an egress IPv6 ACL filter. The Select IPv6 Egress Filter - L3 Access Interface form opens.

16 Choose an egress ACL filter and click on the OK button. The Select IPv6 Egress Filter - L3 Access Interface form closes and the L3 Access Interface (Edit) form reappears with the egress IPv6 ACL filter information displayed.

17 Close the VPRN L3 Access Interface (Edit) form.

18 Click on the OK button to close the VPRN Site (Edit) form.

19 Close the VPRN Service (Edit) form.

20 Close the Manage Services form.

Procedure 71-28 To assign an accounting policy to a VPRN L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Routing Instance icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The VPRN L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Accounting tab.

8 Configure the Collect Accounting Statistics parameter.

9 Click on the Select button to choose an accounting policy. The Select Accounting Policy - L3 Access Interface form opens.

10 Choose an accounting policy and click on the OK button. The Select Accounting Policy - L3 Access Interface form closes and the L3 Access Interface (Edit) form reappears with the accounting policy information displayed.

11 Close the VPRN L3 Access Interface (Edit) form.

12 Click on the OK button to close the VPRN Site (Edit) form.

13 Close the VPRN Service (Edit) form.

14 Close the Manage Services form.

Procedure 71-29 To assign a time of day suite to a VPRN L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Routing Instance icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The VPRN L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the TOD Suite tab.

8 Click on the Select button beside the Name parameter. The Select Time Of Day Suite - L3 Access Interface list form opens.

9 Choose a time of day suite and click on the OK button. The Select Time Of Day Suite - L3 Access Interface list form closes, and the L3 Access Interface (Create) form refreshes with the time of day suite name.

Note 1 — You cannot assign a ToD suite to a L3 access interface if accounting statistics collection is enabled on the interface. You must first disable the Collect Accounting Statistics parameter in step 8 of Procedure 71-28.

Note 2 — SapEgrQosPlcyStats and SapIngQosPlcyStats statistics are collected only if a Time Of Day Suite is applied on the SAP.

10 Close the VPRN L3 Access Interface (Edit) form.

11 Click on the OK button to close the VPRN Site (Edit) form.

12 Close the VPRN Service (Edit) form.

13 Close the Manage Services form.

Procedure 71-30 To bind a VPRN L3 access interface to a VPLS site or VPLS I-site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Routing Instance icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The VPRN L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Routed VPLS tab.

Note 1 — The operational state of the IP interface binding will not be turned up until the Enable IP Interface Binding parameter is set to true.

Note 2 — You can create and manage a routed VPLS connector from the navigation tree on the Composite Service (Edit) form.

8 Enter a VPLS site name or click on the Select button beside the VPLS Name parameter to choose a VPLS site. The Routed VPLS String - VPRN L3 Access Interface form opens.

9 Choose a VPLS site and click on the OK button. The Routed VPLS String - VPRN L3 Access Interface form closes.

10 In the Ingress - IPv4 Filter panel, click on the Select button. The Select IPv4 Filter - VPRN L3 Access Interface form opens.

11 Choose an IPv4 filter and click on the OK button. The Select IPv4 Filter - VPRN L3 Access Interface form closes and the IPv4 filter information is displayed.

12 In the Ingress - IPv6 Filter panel, click on the Select button. The Select IPv6 Filter - VPRN L3 Access Interface form opens.

13 Choose an IPv6 filter and click on the OK button. The Select IPv6 Filter - VPRN L3 Access Interface form closes and the IPv6 filter information is displayed.

14 In the Egress - QoS Policy panel, click on the Select button. The Select QoS Policy - VPRN L3 Access Interface form opens.

15 Choose a QoS Policy and click on the OK button. The Select QoS Policy - VPRN L3 Access Interface form closes and the QoS Policy information is displayed.

16 Close the VPRN L3 Access Interface (Edit) form.

17 Click on the OK button to close the VPRN Site (Edit) form.

18 Close the VPRN Service (Edit) form.

19 Close the Manage Services form.

Procedure 71-31 To associate a local DHCPv4 or DHCPv6 server with a VPRN L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Routing Instance icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The VPRN L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Local DHCP tab and perform one of the following steps.



Note — To associate local DHCPv6 servers the IPv6 Allowed parameter must be enabled.

a For local DHCPv4 servers

i Click on the Select button in the Local DHCP Server panel to choose a local DHCP server. The Select Local DHCP Server - L3 Access Interface form opens.

ii Choose a local DHCP server and click on the OK button. The Select Local DHCP Server - L3 Access Interface form closes, and the L3 Access Interface (Edit) form reappears with the local DHCP server information displayed.

b For local DHCPv6 servers

i Click on the Select button in the Local DHCPv6 Server panel to choose a local DHCPv6 server. The Select Local DHCPv6 Server - L3 Access Interface form opens.

ii Choose a local DHCPv6 server and click on the OK button. The Select Local DHCPv6 Server - L3 Access Interface form closes, and the L3 Access Interface (Edit) form reappears with the local DHCPv6 server information displayed.



Note — You cannot associate a local DHCPv4 server to the L3 group Interface if the Administrative State parameter in the Local Proxy Service panel is up. Go to step 15 of Procedure 71-41 to set the Administrative State.

8 Close the VPRN L3 Access Interface (Edit) form.

9 Click on the OK button to close the VPRN Site (Edit) form.

10 Close the VPRN Service (Edit) form.

11 Close the Manage Services form.

Procedure 71-32 To assign an NE DoS protection policy or NE DDoS protection policy to a VPRN L3 access interface



Note — A default DoS protection policy is automatically assigned to the interface.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Routing Instance icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The VPRN L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Port tab.

8 Click on the Select button in the NE DoS Protection Policy panel and choose a DoS protection policy from the select NE DoS Protection form.

9 Click on the Select button next to the NE DDoS Protection Policy field and choose a DDoS protection policy from the select NE DDoS Protection form.

10 Close the VPRN L3 Access Interface (Edit) form.

11 Click on the OK button to close the VPRN Site (Edit) form.

12 Close the VPRN Service (Edit) form.

13 Close the Manage Services form.

Procedure 71-33 To configure residential subscriber management for a VPRN L3 access interface

Residential subscriber management is supported on the 7450 ESS in mixed mode, 7750 SR, and 7710 SR.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Routing Instance icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The VPRN L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Subscriber Management tab. The Host Connectivity tab is displayed.

8 Select the SHCV Enabled parameter to enable SHCV.

9 Configure the parameters:

- SHCV Interval (minutes)
- SHCV Source
- SHCV Action

10 Close the VPRN L3 Access Interface (Edit) form.

11 Click on the OK button to close the VPRN Site (Edit) form.

12 Close the VPRN Service (Edit) form.

13 Close the Manage Services form.

Procedure 71-34 To assign an IP address to a VPRN L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Routing Instance icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The VPRN L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Addresses tab.

8 Click on the Create button. The IP Address (Create) form opens.

9 Configure the parameters:

- Address ID
- IP Address
- Prefix Length
- Broadcast Address Format
- EUI-64
- IP Address Preferred

The Broadcast Address Format parameter only appears if the IP Address parameter is set to an IPv4 address.

The EUI-64 IP Address Preferred parameters only appear if the IP Address parameter is set to an IPv6 address.

10 Click on the OK button. The IP Address (Create) form closes, and a dialog box appears.

11 Click on the OK button. The VPRN L3 Access Interface (Edit) form reappears with the assigned IP addresses displayed.

12 Close the VPRN L3 Access Interface (Edit) form.

13 Click on the OK button to close the VPRN Site (Edit) form.

14 Close the VPRN Service (Edit) form.

15 Close the Manage Services form.

Procedure 71-35 To configure IPv4 ICMP for a VPRN L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Routing Instance icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The VPRN L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the ICMP tab.

8 Configure the parameters:

- Mask Reply
- Redirects
- Number of Redirects
- Redirects Time (seconds)
- Unreachables
- Number of Unreachables
- Unreachables Time (seconds)
- TTL Expired
- Number of TTL Expired
- TTL Expired Time (seconds)

9 Close the VPRN L3 Access Interface (Edit) form.

10 Click on the OK button to close the VPRN Site (Edit) form.

11 Close the VPRN Service (Edit) form.

12 Close the Manage Services form.

Procedure 71-36 To configure IPv6 ICMP on a VPRN L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Routing Instance icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The VPRN L3 Access Interface (Edit) form opens with the General tab displayed.

7 Ensure that the IPv6 Allowed parameter is enabled.

8 Configure the parameters:

- Redirects
- Number of Redirects
- Redirects Time (seconds)
- Unreachables
- Number of Unreachables
- Unreachables Time (seconds)
- Packet Too Big
- Number of Packet Too Big
- Packet Too Big Time (seconds)
- Param Problem
- Number of Param Problem
- Param Problem Time (seconds)
- Time Exceeded
- Number of Time Exceeded
- Time Exceeded Time (seconds)

9 Close the VPRN L3 Access Interface (Edit) form.

10 Click on the OK button to close the VPRN Site (Edit) form.

11 Close the VPRN Service (Edit) form.

12 Close the Manage Services form.

Procedure 71-37 To configure IPCP for a VPRN L3 access interface

You can configure IPCP only on the ASAP MDA on the 7750 SR and 7710 SR.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Routing Instance icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The VPRN L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the IPCP tab. The IPCP tab is available when the SAP and port is configured with Null or IPCP encapsulation.

8 Configure the parameters:

- Peer Address
- Primary DNS Address
- Secondary DNS Address



Note — Primary and secondary DNS addresses have similar functionality, although they are assigned independently. When both are present, the primary DNS address is used to resolve address names. If the primary DNS address cannot be used the secondary DNS address is used.

9 Click on the OK button. A dialog box appears.

10 Click on the OK button to confirm the action.

11 Close the VPRN L3 Access Interface (Edit) form.

12 Click on the OK button to close the VPRN Site (Edit) form.

13 Close the VPRN Service (Edit) form.

14 Close the Manage Services form.

Procedure 71-38 To configure Bi-directional Forwarding Detection for a VPRN L3 access interface



Note 1 — You cannot configure BFD for an interface if BFD is disabled. See chapter 23 for information about enabling and disabling BFD for routing protocols.

Note 2 — If the IPv6 Allowed parameter in step 7 of Procedure 71-22 is enabled, you can configure the above BFD parameters for IPv6.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Routing Instance icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The VPRN L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the BFD tab. The General tab is displayed.

8 In the IPv4 BFD Configuration panel, set the Admin Status to Up.

9 Configure the parameters:

- Transmit Interval
- Receive Interval
- Echo Interval
- Multiplier
- Termination Type
- Operational State Transition Interval
- Inherit from Network Element

10 In the IPv6 BFD Configuration panel, set the Admin Status to Up.

11 Configure the parameters:

- Transmit Interval
- Receive Interval
- Echo Interval
- Multiplier
- Termination Type
- Operational State Transition Interval
- Inherit from Network Element

12 To view local and remote session peers that are managed by the 5620 SAM, click on the BFD Session tab. A list of BFD current sessions on a router interface or an L3 interface appears.

13 Click on a session. The properties form for the session opens. View the following:

- BFD status
- protocol used
- local address
- remote address
- operational status and statistics

14 Close the form.

15 Close the VPRN L3 Access Interface (Edit) form.

16 Click on the OK button to close the VPRN Site (Edit) form.

17 Close the VPRN Service (Edit) form.

18 Close the Manage Services form.

Procedure 71-39 To configure ARP for a VPRN L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Routing Instance icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The VPRN L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the ARP tab. The General tab is displayed.

8 Configure the Timeout (seconds) parameter.

9 Click on the Create button. The Static ARP (Create) form opens.

10 Configure the parameters:

- Unnumbered
- IP Address
- Physical Address

11 Click on the OK button. The Static ARP (Create) form closes.

12 Click on the Proxy ARP tab.

13 Configure the parameters:

- Remote Proxy ARP
- Enable Local Proxy ARP
- Proxy ARP Policy 1
- Proxy ARP Policy 2
- Proxy ARP Policy 3
- Proxy ARP Policy 4
- Proxy ARP Policy 5

14 Close the VPRN L3 Access Interface (Edit) form.

15 Click on the OK button to close the VPRN Site (Edit) form.

16 Close the VPRN Service (Edit) form.

17 Close the Manage Services form.

Procedure 71-40 To configure neighbor discovery on a VPRN L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Routing Instance icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The VPRN L3 Access Interface (Edit) form opens with the General tab displayed.

7 Set the IPv6 Allowed parameter to enabled.

8 Click on the Neighbor Discovery tab.

9 Click on the Create button. The Neighbor Discovery (Create) form opens.

10 Configure the parameters:

- IP Address
- Physical Address

11 Click on the OK button. A dialog box appears.

12 Click on the OK button. The Neighbor Discovery (Create) form closes, and the L3 Access Interface (Create) form refreshes with the neighbor entry.

13 Click on the Proxy ND tab.

14 Configure the parameters:

- Enable Local Proxy
- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5



Note — Do not leave an empty policy parameter between two configured policy parameters. For example, do not configure the Policy 1 and Policy 3 parameters and leave the Policy 2 parameter unconfigured, or the 5620 SAM reorders the policies and moves the policy specified for the Policy 3 parameter to the Policy 2 parameter.

15 Repeat steps 8 to 14 for each neighbor entry you need to create.

16 Close the VPRN L3 Access Interface (Edit) form.

17 Click on the OK button to close the VPRN Site (Edit) form.

18 Close the VPRN Service (Edit) form.

19 Close the Manage Services form.

Procedure 71-41 To configure IPv4 DHCP for a VPRN L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Routing Instance icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The VPRN L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the DHCP tab. The General tab is displayed.

8 Configure the parameters:

- Enable DHCP Relay
- Description
- Trusted
- Lease Populate
- Enable
- Relay Plain BOOTP
- Use ARP

The Lease Populate parameter is configurable when the Enable parameter is enabled.

9 Depending on the type and release of device that you are configuring, the Subscriber Authentication Policy panel is present. Choose a Subscriber Authentication policy, if required. Otherwise, go to step 14.

10 Click on the Select button in the Subscriber Authentication panel to choose a subscriber authentication policy. The Select Subscriber Authentication Policy - DhcpRelayConfiguration form opens.

11 Click on the Search button.

12 Choose a subscriber authentication policy and click on the OK button. The Select Subscriber Authentication Policy - DhcpRelayConfiguration form closes, and the L3 Access Interface (Create) form refreshes with the subscriber authentication policy name.

13 Configure the parameters:

- Action
- Circuit ID
- Remote ID
- Remote ID String
- Vendor Specific Options
- Vendor String
- IP address
- Use as source
- Relay Unicast Message

The Remote ID String parameter is configurable when the Remote ID is set to Remote ID String.

When the Relay Unicast Message parameter is set to Renew or Release Update Source IP, the GI address parameter can be configured as any local configured address in the same routing instance as the GI address for the DHCP relayed messages. If the Relay Unicast Message parameter is set to None, the GI address is restricted to the IP address configured on the subscriber interface.

14 Click on the Server tab.

15 Configure the parameters:

- Server 1 through Server 8
- Administrative State
- Emulated Server IP Address
- Lease Time
- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time Override

The Number of Days, Number of Hours, Number of Minutes, Number of Seconds, and Lease Time Override parameters are configurable only when the Lease Time parameter is set to Specified Time Period.

16 Close the VPRN L3 Access Interface (Edit) form.

17 Click on the OK button to close the VPRN Site (Edit) form.

18 Close the VPRN Service (Edit) form.

19 Close the Manage Services form.

Procedure 71-42 To create a VRRP instance on a VPRN L3 access interface for a virtual router

You must know the VRID for an existing virtual router and ensure that the interface is a member of the same subnet as the virtual router.

See chapter 33 for configuration information about VRRP instances and virtual routers.



Note — The following configurations are required for the operation of the IPv6 VRRP instance:

- Two tabs are available under the VRRP tab, one for IPv4 instances and the other for IPv6 instances. You can only create an IPv6 VRRP Instance if you enable the IPv6 Allowed parameter on the General tab of the VPRN L3 Access Interface (Edit) form.
- The Link Local Address on the parent interface must be set to preferred and configured as one of the backup addresses (or same subnet) for the IPv6 VRRP instance. The Admin Link Local Address and Admin Link Local Address Preferred parameters on the General tab of the VPRN L3 Access Interface (Edit) form must be set accordingly.
- The IPv6 address on the parent interface must be set to preferred to be used as a backup address (on same subnet) for the IPv6 VRRP instance. The IP Address and IP Address Preferred parameters in step 9 of Procedure 71-34 must be set accordingly.
- The Send Advertisement and Use Virtual MAC Address parameters must be enabled in step 9 of Procedure 71-44 for the router advertisement on the parent interface.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Routing Instance icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The VPRN L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the VRRP tab.

8 Click on the Create button. The VRRP Instance (Create) form opens with the General tab displayed.

9 Configure the Virtual Router ID parameter.

10 Perform steps 8 to 15 of Procedure 33-2.



Note — You can use the VR Instances tab to create, modify, and view VR instances.

11 Click on the OK button. The VRRP Instance (Create) closes and the L3 Access Interface (Edit) form reappears.

12 Close the VPRN L3 Access Interface (Edit) form.

13 Click on the OK button to close the VPRN Site (Edit) form.

14 Close the VPRN Service (Edit) form.

15 Close the Manage Services form.

Procedure 71-43 To configure anti-spoofing filters for a VPRN L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Routing Instance icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The VPRN L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Anti-Spoofing tab.

8 Configure the parameters:

- Anti-Spoofing
- ARP Populate

The ARP Populate parameter is configurable when all of the IP addresses of the defined static hosts on the interface are in one of the subnets configured for the interface.

9 Click on the Static Hosts tab to configure static subscriber host entries, if subscriber entries are not available through DHCP lease management.

10 Click on the Create button. The Access Interface Anti-Spoofing Static Host Display (Create) form opens.

11 Configure the parameters:

- IP Address
- MAC Address

Specify at least one IP address or MAC address for each static host. The values specified for the Anti-Spoofing and ARP Populate parameters determine the type of address entry that is required for the static host. For example, when you set the Anti-Spoofing parameter to Source Ip Addr, you must specify at least the IP address for the static host.



Note — You can configure a static host on a SAP only when no static ARP entries exist on the IP interface.

When the ARP Populate parameter is enabled, the IP address of the new static host must be in one of the subnets that is configured for the interface in Procedure 71-34.

12 Click on the Apply button if you need to create additional entries. A dialog box appears. Otherwise, go to step 15.

13 Click on the OK button.

14 Repeat steps 11 to 13 to create additional entries, if required.

15 Click on the OK button. A dialog box appears.

16 Click on the OK button. The Access Interface Anti-Spoofing Static Host Display (Create) form closes and the Static Hosts tab refreshes with the configured static hosts displayed.

17 Close the VPRN L3 Access Interface (Edit) form.

18 Click on the OK button to close the VPRN Site (Edit) form.

19 Close the VPRN Service (Edit) form.

20 Close the Manage Services form.

Procedure 71-44 To configure router advertisement on a VPRN L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Routing Instance icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The VPRN L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Advertisement tab.

8 Click on the Create button to add a router advertisement entry. The Router Advertisement (Create) form opens.

9 Configure the parameters:

- Send Advertisement
- Min Interval (seconds)
- Reachable Time (milliseconds)
- Managed Address Config
- MTU
- Use Virtual MAC Address
- Max Interval (seconds)
- Retransmit Time (milliseconds)
- Other Stateful Config
- Current Hop Limit
- Lifetime (seconds)

If you are configuring the L3 interface for an IPv6 VRRP instance, then the Send Advertisement and Use Virtual MAC Address parameters must both be enabled.

10 Click on the Prefix tab.

11 Click on the Create button. The Router Advertisement Prefix (Create) form opens.

12 Configure the parameters:

- IPv6 Prefix
- On-Link Determination
- Prefix Length
- Autonomous Address Configuration
- Lifetime (seconds) in Preferred Lifetime panel
- No Expiry in Preferred Lifetime panel
- Lifetime (seconds) in Valid Lifetime panel
- No Expiry in Valid Lifetime panel

13 Click on the OK button. A dialog box appears.

14 Click on the OK button. The Router Advertisement (Create) form reappears.

15 Click on the OK button. A dialog box appears.

16 Click on the OK button. The Router Advertisement (Create) form closes and the VPRN L3 Access Interface (Edit) form refreshes with the router advertisement entry.

17 Close the VPRN L3 Access Interface (Edit) form.

18 Click on the OK button to close the VPRN Site (Edit) form.

19 Close the VPRN Service (Edit) form.

20 Close the Manage Services form.

Procedure 71-45 To assign an ANCP policy to a VPRN L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Routing Instance icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The VPRN L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the ANCP Static Map tab.

8 Click on the Create button. The ANCP Static Map (Create) form opens with the General tab displayed.

9 Configure the ANCP String parameter.

10 Click on the Select button in the ANCP Policy panel to choose an ANCP policy. The Select ANCP Policy - ANCP Static Map list form opens.

11 Choose an ANCP policy and click on the OK button. The Select ANCP Policy - ANCP Static Map form closes and the ANCP Static Map form reappears with the ANCP policy information displayed.

12 Click on the OK button. A dialog box appears.

13 Click on the OK button. The ANCP Static Map (Create) form closes.

14 Close the VPRN L3 Access Interface (Edit) form.

15 Click on the OK button to close the VPRN Site (Edit) form.

16 Close the VPRN Service (Edit) form.

17 Close the Manage Services form.

Procedure 71-46 To specify queue overrides on a VPRN L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Routing Instance icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The VPRN L3 Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Override Policy Items tab.



Note — The Override Policy Items tab contains a number of tabs. However, the tabs that are displayed depend on the port type that you have chosen for this interface.

- If you configured a non-HSMDA port, then the Access Ingress Queues, Access Egress Queues, Ingress Policer, and Egress Policer tabs are active.
- If you configured an HSMDA port, then the Access Ingress Queues, Access Egress HSMDA Queues and Ingress Policer tabs are active.

Set the queue overrides, as described in Procedure 43-42.

8 Close the VPRN L3 Access Interface (Edit) form.

9 Click on the OK button to close the VPRN Site (Edit) form.

10 Close the VPRN Service (Edit) form.

11 Close the Manage Services form.

Procedure 71-47 To configure IPv6 DHCP on a VPRN L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Expand the Sites icon in the service navigation tree.

5 Expand the Routing Instance icon in the service navigation tree on which you need to configure the L3 access interface.

6 Right-click on the L3 Access Interface icon and choose Properties from the contextual menu. The VPRN L3 Access Interface (Edit) form opens with the General tab displayed.

7 Set the IPv6 Allowed parameter to enabled.

8 Click on the DHCPv6 tab. The General tab is displayed.

9 Configure the parameters:

- Enable DHCPv6 Relay
- Description
- Lease Populate
- Maximum Number of Leases
- Route Populate PD
- Route Populate PD Exclude
- Route Populate NA
- Route Populate TA
- Interface Id Option
- Interface Id String
- Remote ID
- Source IP Address
- Neighbor Resolution
- Prefix Option

10 Click on the Server tab.

11 Configure the Server 1 through Server 8 parameters.

12 Configure the interface name for each DHCPv6 server that you configured in step 11 by clicking on the Select button in the Zone Index panel. The Select Zone Index - DhcpRelayV6Configuration form opens with a list of configured interfaces.

13 Choose an interface and click on the OK button. The Select Zone Index - DhcpRelayV6Configuration list form closes and the L3 Access Interface form refreshes with the interface information.

14 Click on the DHCPv6-Prefix tab.

15 Click on the Create button. The DhcpRelayV6PrefixDelegation (Create) form opens.

16 Configure the parameters:

- Prefix Address
- Prefix Length
- Prefix DUID
- Prefix IAID
- Prefix Life Time (seconds)
- Prefix Valid Life Time (seconds)

17 Click on the OK button. A dialog box appears.

18 Click on the OK button. The VPRN L3 Access Interface (Edit) form reappears.

19 Close the VPRN L3 Access Interface (Edit) form.

20 Click on the OK button to close the VPRN Site (Edit) form.

21 Close the VPRN Service (Edit) form.

22 Close the Manage Services form.

Procedure 71-48 To configure a VPRN network interface



Note — You cannot configure at network interface on a VPRN service if there are any pre-existing interfaces configured on the service. Once a network interface is configured on a VPRN service, no other interface types can be configured on the service.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service.

4 Click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

5 Click on the Sites tab.

6 Choose a VPRN site and then click on the Properties button. The VPRN Site (Edit) form opens with the General tab displayed.

7 Click on the Routing tab. The General tab is displayed.

8 Configure the Carrier Carrier VPN parameter.

The Carrier Carrier VPN parameter is only available if there are no other interfaces configured on the site.

9 Click OK on the VPRN Site (Edit) form. The VPRN Site (Edit) form closes and the VPRN Service (Edit) form reappears.

10 Click on the Network Interfaces tab and then click on the Create button. The Network Interface (Create) form opens with the General tab displayed.

11 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- MAC Address
- Allow Directed Broadcasts
- Class
- Loopback Enabled
- PIM RP Delayed Up Period
- Cflowd Type
- Trusted
- Enable Ingress Flowspec
- Enable Ingress Stats
- LSR IP Load Balancing
- URPF Check State IPv4
- URPF Check Mode IPv4
- URPF Check State IPv6
- URPF Check Mode IPv6
- Broadcast

The URPF Check State IPv6 and URPF Check Mode IPv6 parameters are only configurable when the IPv6 Allowed parameter is enabled.



Note — When the Broadcast parameter is enabled, a time protocol such as NTP or SNTP must be enabled and configured on the device, or the device ignores broadcast time packets received on the interface. See chapter 9 for information about configuring NTP or SNTP on a device.

12 Click on the Port tab.



Note — If the Loopback Enabled parameter is selected on the General tab, the Port port tab does not appear. Skip to step 15.

13 Click on the Select button and select a terminating port for the interface from the Select Terminating Port form.

14 Configure the parameters:

- Outer Encapsulation Value
- Auto-Assign ID
- Inner Encapsulation Value



Note — If you Clear or change the port associated with an existing Network Interface, the Network Policy associated to the Network Interface will remain but all the redirect information will be cleared. This includes the Egress Queue Group Template Policy and its Egress Queue Group Instance ID, as well as the Ingress Queue Group Template Policy and its Ingress Queue Group Instance ID. These will subsequently need to be reconfigured if required.

15 Click on the Policies tab.

i In the Network Policy panel, click on the Select button in the Network Policy panel to list and choose a network policy for the interface. Network policies are used to determine QoS settings based on the packet DSCP bits on the ingress and egress of the network.



Note 1 — If you select a network policy with a forwarding class mapped to a queue group queue ID, you must ensure that the mapping queue group queue ID is in the selected Queue Group Template Policy.

See Procedure 16-1 for more information about how to configure Ethernet ports. See chapter 42 for more information about queue group template policies.

Note 2 — If you need to add a Port Redirect Group (policer) to any of the Ingress Forwarding Classes in the the global copy of the Network Policy, you must first define the policer in the global copy of the Ingress Queue Group Template Policy.

Note 3 — If you need to add a Port Redirect Group (queue or policer) to any of the Egress Forwarding Classes in the the global copy of the Network Policy, you must first define the queue or policer in the global copy of the Egress Queue Group Template Policy.

ii In the Ingress Forwarding Plane Redirect panel, click on the Select button to choose a queue group template policy for the interface's ingress forwarding plane redirection. Only global Ingress Queue Group Template Policies that have already been defined can be chosen. Queue group template policies allow SAP or IP interface forwarding classes to be redirected from the typical queue mapping to a shared queue.

iii Configure the Queue Group Instance ID parameter.



Note 1 — You must ensure that the port you selected in step 13 has a network egress queue group with the same name as the Queue Group Template policy created on it.

Note 2 — If the Network Policy you selected in step i has Port Redirect Groups on its Ingress Forwarding Classes, you must specify both an Ingress Queue Group Template Policy and Instance ID.

Note 3 — If the Network Policy you selected in step i has Port Redirect Groups on its Ingress Forwarding Classes, these must already be defined within the Ingress Queue Group Template Policy you select.

Note 4 — If you need to remove an existing Port Redirect Group (policer) from any of the Ingress Forwarding Classes in the the global copy of the Ingress Queue Group Template Policy, you must first remove the policer in the global copy of the Network Policy.

Note 5 — Queue Group Template policies are not applicable to L3 interfaces associated with HSMDA ports.

See Procedure 16-1 for more information about how to configure Ethernet ports. See chapter 42 for more information about queue group template policies.

iv In the Egress Port Redirect panel, click on the Select button to choose a queue group template policy for the interface's egress port redirection. Only local Egress Queue Group Template Policies which have a Network Egress Queue Group Instance defined on the associated port can be chosen.

v Configure the Queue Group Instance ID parameter.



Note 1 — If the Network Policy you selected in step i has Port Redirect Groups on its Egress Forwarding Classes, you must specify both an Egress Queue Group Template Policy and Instance ID.

Note 2 — If the Network Policy you selected in step i has Port Redirect Groups on its Egress Forwarding Classes, these must already be defined within the Egress Queue Group Template Policy you select. The default policy does not contain any redirects.

Note 3 — If you need to remove an existing Port Redirect Group (queue or policer) from any of the Egress Forwarding Classes in the the global copy of the Egress Queue Group Template Policy, you must first remove the queue or policer in the global copy of the Network Policy.

Note 4 — Queue Group Template policies are not applicable to L3 interfaces associated with HSMDA ports.

See Procedure 16-1 for more information about how to configure Ethernet ports. See chapter 42 for more information about queue group template policies.

vi Click on the Select buttons to list and choose Ingress and Egress ACL filters for the interface. ACL filters are used to filter out IP traffic that matches user-defined criteria.

16 Assign a DoS protection policy or DDoS protection policy to the interface, if required.



Note — A default DoS protection policy is automatically assigned to the interface.

i Click on the Security tab.

ii Click on the Select button beside the DoS Policy ID field and select a policy from the Select NE DoS Protection form.

iii Click on the Select button beside the NE DDoS Protection Policy field and select a policy from the Select NE DDoS Protection Policy form.

17 Configure Bi-directional Forwarding Detection for the interface, if required.

i Click on the BFD tab.

ii Configure the parameters:

- Administrative State
- Transmit Interval
- Receive Interval
- Echo Interval
- Multiplier
- Termination Type
- Operational State Transition Interval
- Inherit from Network Element

The Transmit Interval, Receive Interval, Receive Interval, Echo Interval, Multiplier, Termination Type, Operational State Transition Interval, and Inherit from Network Element parameters are configurable only when the Administrative State parameter is set to Up.

iii To view local and remote session peers that are managed by the 5620 SAM. Click on the BFD Session tab. A list of BFD current sessions on the interface appears.

iv Click on a session. The properties form for the session opens. View the following:

- BFD status
- protocol used
- local address
- remote address
- operational status and statistics

v Close the form.



Note — You cannot configure BFD for an interface if BFD is disabled. See chapter 23 for information about enabling and disabling BFD for routing protocols.

18 Click on the ARP tab.

i Configure the Timeout (seconds) parameter.

ii Click on the Create button to statically associate an IP or MAC address to the interface. The Static ARP (Create) form opens.

Configure the parameters:

- IP Address
- Physical Address

iii Click on the OK button. The Static ARP (Create) form closes.

19 Click on the Addresses tab to assign IP addresses to the interface:

i Click on the Create button. The IP Address, Routing Instance (Create) form opens.

ii Configure the parameters:

- Address ID
- IP Address
- Prefix Length
- IGP Inhibit
- Broadcast Address Format

iii Click on the OK button to save the changes. A dialog appears.

iv Click on the OK button. The IP Address, Routing Instance (Create) form closes. The Network Interface (Create) form reappears with the assigned IP addresses displayed.

20 Click on the ICMP tab and configure the parameters:

- Mask Reply
- Redirects
- Unreachables
- TTL Expired
- Number of Redirects
- Redirects Time (seconds)
- Number of Unreachables
- Unreachables Time (seconds)
- Number of TTL Expired
- TTL Expired Time (seconds)

21 Click on the OK button. The Network Interface [Create] form closes. The VPRN Service (Create) form reappears with the assigned network interface displayed.

Procedure 71-49 To configure a GNE site on a VPRN service

Use this procedure to add a GNE site and GNE service interfaces to an existing VPRN service.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

4 On the component tree, right-click on VPRN Service and choose Create GNE Site. The Select Network Elements - VPRN Service form opens with a list of available sites.

5 Choose a site and click on the OK button. The GNE Site (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Name
- Description

7 Click on the Apply button.

8 To configure an interface for the GNE site, perform the following steps:

i Click on the GNE Service Interfaces tab and then click on the Create button. The GNE Service Interface (Create) form opens with the general tab displayed.

ii Configure the parameters:

- Name
- Description
- Type

iii Click on the Ports tab and then click on the Select button beside the Interface Index field. The Select Generic NE Interface form opens.

iv Choose an interface and click on the OK button. The GNE Service Interface (Create) form reappears with the interface information displayed.

v Configure the parameters:

- Encapsulation Type
- Outer Encapsulation Value
- Inner Encapsulation Value

vi Click on the OK button. The GNE Site (Create) form reappears with the interface information displayed in the service component tree.

9 Click on the Scripts tab to attach or execute configuration scripts on the GNE site.

The Scripts tab displays the script instances and versions that are applied to the device. See “Script management” in the *5620 SAM Scripts and Templates Developer Guide* for more information.

10 Click on the OK button. The VPRN Service (Edit) form reappears with the new information displayed in the service component tree.

11 Click on the OK button. The VPRN Service (Edit) form closes.

You can use the topology maps to view the service. See chapter 6 for more information about service topology maps.

Procedure 71-50 To configure OSPFv2, OSPFv3, PIM, RIP, L2TP, or MLD on a VPRN routing instance

Note 1 — To configure BGP on a VPRN routing instance, see Procedure 71-51.

Note 2 — To configure IGMP on a VPRN routing instance, see Procedure 71-52.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service.

4 Click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

5 On the navigation tree, click on the site to which you need to add the routing instance; expand the entries for that site.

6 Expand the Routing Instance - NE System ID icon.

7 Expand the Routing Instance icon.

8 Right-click on the Protocols icon and perform one of the following from the contextual menu:

   a Choose Create OSPF Site to configure OSPFv2 on the VPRN routing instance, and perform steps 4 to 18 of Procedure 23-30.

   b Choose Create OSPF Site to configure OSPFv3 on the VPRN routing instance, and perform steps 4 to 10 and steps 12 to 18 in Procedure 23-30.

   c Choose Create PIM Site to configure PIM on the VPRN routing instance, and perform steps 9 to 83 in Procedure 23-41.

   d Choose Create RIP Site to configure RIP on the VPRN routing instance, and perform steps 4 to 15 in Procedure 23-9.

   e Choose Create L2TP Site to configure L2TP on the VPRN routing instance, and perform steps 3 to 14 in Procedure 23-34.

   f Choose Create MLD Site to configure MLD on the VPRN routing instance, and perform steps 2 to 6 in Procedure 23-59.

Note — You must ensure that the VPRN routing instance has an associated L3 access interface, and that the IPv6 Allowed parameter on the interface is enabled. You must add an IPv6 address to the L3 access interface. See Procedures 71-22 and 71-34.

9 Click on the OK button. The protocol configuration form closes, and a dialog box appears.

10 Click on the OK button. The VPRN Service (Edit) form reappears.

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button to confirm the action. The VPRN Service (Edit) form closes.

13 Close the Manage Services form.

Procedure 71-51 To configure BGP on a VPRN routing instance

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service.

4 Click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

5 Expand the Routing Instance icon in the navigation tree.

6 Right-click on the site on which you need to configure BGP and choose Properties from the contextual menu.

7 Click on the Routing tab. The Protocols tab is displayed.

8 Enable the BGP Enabled parameter on the Protocols tab. A list of BGP routing instances appears.

9 Choose a routing instance and click on the Properties button. The BGP Site, Routing Instance (Create) form opens with the General tab displayed.

10 Configure the parameters:

- Description
- Router ID
- Administrative State
- Cluster ID

11 Assign a TCP key chain, if required.



Note — You can assign a TCP key chain to a BGP site, group, or peer on a 7950 XRS, 7750 SR, or on a 7450 ESS in mixed mode.

i Click on the Select button in the KeyChain panel. The Select BGP Site Keychain - BGP form opens.

ii Choose a key chain in the list and click on the OK button. The Select BGP Site Keychain - BGP form closes. The 5620 SAM assigns the key chain to the BGP instance.

12 Configure the parameters in the Graceful Restart panel:

- Graceful Restart
- Stale Routes Time (seconds)
- Enable Notification

The graceful restart parameters are configurable when you enable the Graceful Restart parameter.

13 Configure the parameters in the MED panel:

- MED Source
- MED Value

These parameters are used to find a way to leave the AS when there are multiple methods of leaving the AS.

14 Configure the parameters in the MultiPath panel:

- Multi Path
- IBGP MultiPath

Set the Multi Path parameter to 1 to disable. When set from 2 to 16, multipath is enabled and BGP load shares traffic across the number of links specified. If the equal cost routes available are greater than the configured value, then routes with the lowest next hop IP address are chosen.

15 Configure the EIBGP Load Balance parameter in the EIBGP LoadBalance panel.

16 Configure the Backup Path parameter in the Backup Path panel.

17 Configure the parameters in the Best Path Selection panel:

- Ignore Next Hop Metric
- Ignore Router Id
- MED Compare
- Deterministic MED
- Strict

When you set the MED Compare parameter to off, the Strict parameter is set to true and is not configurable. When you set the MED Compare parameter to on, the Strict parameter is set to false and is not configurable.

18 Click on the Behavior tab.

19 Configure the parameters:

- Preference
- Local Preference
- Multi Hop
- Loop Detect
- Aggregator ID Zero
- Damping
- Disable Client Reflect
- Min. Route Advertisement
- Disable Standard Communities
- Disable Extended Communities
- Disable Fast External Failover
- Advertise Inactive Routes
- Enable Rapid Withdrawal
- Enable Peer Tracking
- BFD Enabled
- FlowSpec Validate Enabled
- Connect Retry Time (seconds)
- Keep Alive (seconds)
- Transport Tunnel
- Path MTU Discovery Enabled
- Split Horizon

20 Configure the Policy parameter in the Next-Hop Resolution panel.

21 Configure the parameters in the Hold Time panel:

- Hold Time (seconds)
- Minimum Hold Time (seconds)

22 Configure the Fault Tolerance parameter in the Error Handling panel. The Fault Tolerance parameter allows BGP routers to be more tolerant of some Update message errors, use less disruptive error recovery mechanisms, and provide better operational and diagnostics information.

23 Configure the parameters in the Damp Peer Oscillations panel:

- Enable Damp Peer Oscillation
- Initial Wait Time (minutes)
- Second Wait Time (minutes)
- Maximum Wait Time (minutes)
- Error Interval (minutes)

24 Click on the AS Properties tab.

25 Configure the parameters:

- Min AS Origination (seconds)
- Disable 4Byte ASN

26 Configure the parameters in the Local AS panel:

- Local AS
- Private
- No Prepend Global AS

The No Prepend Global AS is configurable only if you set the Local AS parameter to a value other than 0.

The Local AS parameters are used to configure a virtual AS. A virtual AS is used when a router (RTA) is moved from one AS (AS1) to another AS (AS2). However, the customer router (CR1) is configured to belong to the AS1. To avoid reconfiguring CR1 to belong to AS2, CR1 can continue to belong to AS1, but RTA has its local AS value set to AS1. RTA can advertise AS1 for routes advertised to CR1.

27 Configure the parameters in the Remove Private AS panel:

- Remove Private AS
- Limited

28 Click on the VPN tab.

29 Configure the parameters:

- Family
- Apply Import Route Policies
- Apply Export Route Policies



Note 1 — The Apply Import Route Policies and Apply Export Route Policies parameters are not supported on a VPRN BGP instance.

Note 2 — The Apply Import Route Policies and Apply Export Route Policies parameters specify whether to apply the existing import and export route policies configured on the Import Policies and Export Policies tabs.

30 Add a group, if required.

i Click on the Group tab.

ii Click on the Create button. The Peer Group (Create) form opens with the General tab displayed.

iii Perform steps 4 to 31 of Procedure 23-4.

31 Add a peer, if required.

i Click on the Peer tab.

ii Click on the Create button. The Peer (Create) form opens.

iii Perform steps 4 to 31 of Procedure 23-5.

32 Click on the Import Policies tab.

33 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5
- Policy 6
- Policy 7
- Policy 8
- Policy 9
- Policy 10
- Policy 11
- Policy 12
- Policy 13
- Policy 14
- Policy 15

Configure the import route policies to determine which routes are accepted from peers. These policies should match the policies you configure using the Routing Policy Manager, as described in chapter 22. The router does not validate to ensure that the policies match.

34 Click on the Export Policies tab.

35 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5
- Policy 6
- Policy 7
- Policy 8
- Policy 9
- Policy 10
- Policy 11
- Policy 12
- Policy 13
- Policy 14
- Policy 15

Configure the export route policies to determine which routes are advertised to peers. These policies should match the policies you configure using the Routing Policy Manager, as described in chapter 22. The router does not validate to ensure that the policies match.

36 Click on the Authentication tab.

37 Configure the parameters:

- Type
- Key

38 Click on the OK button. A dialog box appears.

39 Click on the Yes button. The VPRN Site (Edit) form reappears.

40 Click on the OK button. A dialog box appears.

41 Click on the Yes button. The VPRN Service (Edit) form closes.

42 Close the Manage Services form.

Procedure 71-52 To configure IGMP on a VPRN routing instance



Note — PIM-SSM for IPv6 is currently not supported in VPRN services.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service.

4 Click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

5 On the navigation tree, click on the site to which you need to add the routing instance; expand the entries for that site.

6 Expand the Routing Instance icon.

7 Right-click on the Protocols icon and choose Create IGMP Site from the contextual menu. The IGMP Site (Edit) form opens with the General tab displayed.

8 Configure the parameters:

- Administrative State
- Query Interval (seconds)
- Last Member Query Interval (seconds)
- Query Response Interval (seconds)
- Robust Count
- Group Interface Query Source IP

9 Click on the SSM Translation tab to configure SSM, if required.

i Click on the Create button to create a new entry. The SSM Translation (Create) form opens.

ii Configure the parameters:

- Start Mcast Address
- End Mcast Address
- Configured Source

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The new SSM entry appears on the form.

10 Click on the Interfaces tab to add an interface, if required.

i Click on the Create button.

ii Perform steps 4 to 14 of Procedure 23-48.

iii Click on the OK button. The new interface entry appears on the form.

11 Click on the Group Interfaces tab to identify an IGMP group interface for a VPRN service, if required.

i Click on the Create button. The IGMP Group Interface - Routing Instance (Create) form opens with the General tab displayed.

ii Configure the parameters:

- Description
- Query Source IP
- Administrative State
- Administrative Version
- Forwarding Service ID

iii Click on the Select button beside the Interface ID field in the IGMP Group Interface panel to choose an IGMP group interface.

iv Choose an IGMP group interface and click on the OK button. The Select IGMP Group Interface form closes and the IGMP Group Interface - Routing Instance (Create) form reappears.

v Configure the parameters:

- Maximum Number of Groups
- Maximum Number of Sources
- Maximum Number of Group Sources

vi Click on the Multicast CAC tab, if required. The General tab is displayed.

vii Click on the Select button in the Multicast CAC Policy panel. The Select Multicast CAC Policy - IGMP Interface Group form opens.

viii Choose a multicast CAC policy and click on the OK button. The Select Multicast CAC Policy - IGMP Group Interface form closes and the IGMP Interface, Routing Instance (Create) form opens.

ix Configure the parameters:

- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)
- Constraint Admin State

x Click on the OK button to close the IGMP Group Interface - Routing Instance (Create) form. The Group Interfaces tab reappears.

12 Click on the following tabs to view and edit information.

- Multicast Group/Source
- Statistics
- Faults

13 Click on the OK button. The protocol configuration form closes, and a dialog box appears.

14 Click on the OK button. The VPRN Service (Edit) form reappears.

15 Click on the OK button. A dialog box appears.

16 Click on the Yes button to confirm the action. The VPRN Service (Edit) form closes.

17 Close the Manage Services form.

Procedure 71-53 To add a Global Route Table to a VPRN site

Packets within a VRF are able to perform a parallel lookup against a Global Route Table (GRT), as well as within the local VRF. A successful routing table match found in the local VRF is typically preferred over any match found in the GRT. However, a static route can be used to allow for specific prefixes covered by the static route to fail the lookup in the local VRF table, thus resulting in the guaranteed use of a route from the GRT.

The GRT is populated by defining export policies for each participating VPRN service, and the maximum number of routes that are exported from a specific VRF can be limited.



Note — The addition of a GRT to a VPRN service is supported on the 7450 ESS in mixed mode, 7710 SR, and 7750 SR.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose the required VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site to which you need to add the GRT; expand the entries for that site.

5 Right-click on the routing instance to which you need to add the GRT and select Properties. The VPRN Site (Edit) form opens with the General tab displayed.

6 Click on the Routing tab. The General tab is displayed.

7 Configure the Enable GRT Lookup parameter.

8 Click on the GRT Export Policies .

9 Configure the parameters:

- Max Number of Exported Routes
- Max Number of IPv6 Exported Routes

10 Specify up to five export policies by using the Select button to choose policies from the filtered list and then clicking on the OK button.

11 Click on the OK button. A dialog box appears.

12 Click on the OK button. The VPRN Site (Edit) form closes and a dialog box appears.

13 Click on the OK button. The VPRN Service (Edit) form closes.

14 Close the Manage Services form.

Procedure 71-54 To add a PIM interface to a VPRN

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service.

4 Click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

5 On the navigation tree, click on the site to which you need to add the PIM; expand the entries for that site.

6 Expand the Routing Instance icon.

7 Expand the Protocols icon.

8 Right-click on a PIM instance in the service navigation tree and choose Create PIM Interface. The PIM Interface, Routing Instance (Create) form opens.

9 Assign an L3 access interface to the PIM interface by clicking on the Select button in the Interface panel. The Select Interface - PIM Interface form opens.

10 Configure the filter criteria. A list of available L3 access interfaces appears at the bottom of the Select Interface - PIM Interface form.

11 Choose an interface and click on the OK button. The Select Interface - PIM Interface form closes and the PIM Interface, Routing Instance (Create) form refreshes with the L3 access interface information.

12 Configure the parameters:

- Description
- Administrative State
- BFD Enabled

13 Click on the Behavior tab.

14 Configure the parameters:

- Hello Interval (seconds)
- Tracking Support
- BSM Check Router Alert
- Improved assert
- Max Groups
- Three Way Hello
- Multicast Senders
- Hello Multiplier
- Assert Period
- DR Priority
- Sticky DR
- Sticky DR Priority
- P2MP to LDP Tree Join Enabled

The Sticky DR Priority parameter is configurable when the Sticky DR parameter is enabled.

15 Click on the Multicast CAC tab to add a multicast CAC policy, if required. The General tab is displayed.

16 Click on the Select button in the Multicast CAC Policy panel to choose a multicast CAC policy. The Select Multicast CAC Policy - PIM Interface form opens.

17 Choose a multicast CAC policy and click on the OK button. The Select Multicast CAC Policy - PIM Interface form closes and the PIM Interface, Routing Instance (Create) form refreshes with the multicast CAC policy information.

18 Configure the parameters:

- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)
- Constraint Admin State

19 Click on the OK button. A dialog box appears.

20 Click on the OK button.

21 Click on the OK button to close the VPRN Service (Edit) form. A dialog box appears.

22 Click on the Yes button to confirm the action. The VPRN Service (Edit) form closes.

23 Click on the Close button to close the Manage Services form.

Procedure 71-55 To add an IGMP interface to a VPRN



Note — IGMP must be enabled at the routing instance level before you can create an IGMP interface.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site to which you need to add the IGMP interface; expand the entries for that site.

5 Right-click on an IGMP instance and choose Create IGMP Interface. The IGMP interface, Routing Instance (Create) form opens with the General tab displayed.

6 Assign an L3 access interface to the PIM interface by clicking on the Select button in the Interface panel. The Select Interface - PIM Interface form opens.

7 Configure the filter criteria. A list of available L3 access interfaces appears at the bottom of the Select Interface - PIM Interface form.

8 Choose an interface and click on the OK button. The Select Interface - PIM Interface form closes and the PIM Interface, Routing Instance (Create) form refreshes with the L3 access interface information.

9 Configure the parameters:

- Description
- Administrative State
- Administrative Version

10 Click on the Behavior tab.

11 Configure the parameters:

- Import Policy
- Maximum Number of Groups
- Maximum Number of Sources
- Maximum Number of Group Sources
- Subnet Check
- Disable Router Alert Check
- Sub Hosts Only

12 Click on the Multicast CAC tab to add a multicast CAC policy, if required.

13 Click on the Select button in the Multicast CAC Policy panel to choose a multicast CAC policy. The Select Multicast CAC Policy - IGMP Interface form opens.

14 Choose a multicast CAC policy and click on the OK button. The Select Multicast CAC Policy - IGMP Interface form closes and the IGMP Interface, Routing Instance (Create) form refreshes with the multicast CAC policy information.

15 Configure the parameters:

- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)
- Constraint Admin State

16 Click on the Static Group/Source tab to add a static multicast group or source, if required.

17 Click on the Create button to add a new entry. The StaticGrpSrc, Routing Instance (Create) form opens.

18 Configure the parameters:

- Static Multicast Group
- Static Source

19 Click on the OK button. The StaticGrpSrc, Routing Instance (Create) form closes and a dialog box appears.

20 Click on the OK button to confirm the action.

21 Click on the OK button to close the IGMP Interface, Routing Instance (Create) form. A dialogue box opens.

22 Click on the OK button to confirm the action. The VPRN Service (Edit) form reappears.

23 Click on the OK button to close the VPRN Service (Edit) form. A dialog box appears.

24 Click on the Yes button to confirm the action. The VPRN Service (Edit) form closes and the Manage Services form reappears.

25 Close the Manage Services form.

Procedure 71-56 To create a VPRN spoke SDP binding

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN and click on the Properties button. The VPRN Service (Edit) form opens.

4 On the navigation tree, click on the site to which you need to add the spoke SDP binding; expand the entries for that site.

5 Right-click on Spoke SDP Bindings and choose Create Spoke SDP Binding from the contextual menu. The Spoke SDP Binding (Create) form opens with the General tab displayed.

6 Specify a source interface for the SDP binding:

i Click on the Select button in the Source Interface panel. The Select Source Interface - Spoke SDP Binding form opens.

ii Configure the filter criteria. A list of interfaces appears at the bottom of the form.

iii Choose an interface and click on the OK button. The Select Source Interface - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the source interface information.

After you choose the interface, other tabs are also displayed on the form.

7 Configure the parameters:

- VC ID
- Auto-Assign ID
- VC Type
- Enable Ingress FlowSpec IPv4
- Enable Ingress FlowSpec IPv6

These parameters appear only when a source interface is assigned to the spoke SDP binding.

8 Configure the parameters in the Hash Label panel:

- Enable Hash Label
- Enable Signal Capability

The Enable Hash Label and Enable Signal Capability parameters can only be configured for spoke-SDP bindings that are access interface terminated.

9 Specify a destination node for the spoke SDP binding:

a If the destination node is a managed NE:

i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element - Spoke SDP Binding form opens.

ii Choose a destination node and click on the OK button. The Select Destination Network Element - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the tunnel termination site (the destination node) identifier displayed.

b If the destination node is an unmanaged NE, specify its system ID in the Tunnel Termination Site parameter.

10 Configure the Description parameter.

11 Perform one of the following to specify a transport tunnel for the spoke SDP binding:

a For the 5620 SAM to configure the transport tunnel automatically.

i Enable the Auto-Select Transport Tunnel parameter.

ii Configure the Profile Name or the Tunnel Auto-Selection Transport Preference parameter.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens.

ii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier.

c Configure an MPLS-TP transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens.

ii Select an MPLS-TP service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier. See Procedure 27-1 for more information about how to create an MPLS-TP service tunnel.

12 Specify an application profile for the spoke SDP binding.

i Click on the Select button beside the Application Profile parameter. The Application Profile String: - Spoke SDP Binding form opens.

ii Configure the filter criteria. A list of application profiles appears.

iii Choose an application profile and click on the OK button. The Application Profile String: - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form opens.



Note — The Application Profile String: - Spoke SDP Binding - VPRN service form displays only local profiles on the NE.

13 Choose one of the following AA transit policy types, if required.



Note 1 — You can only associate one AA transit policy type with a service object.

Note 2 — You can bind a transit policy to only one L3 access interface or spoke SDP binding per node.

Note 3 — The transit policy and the application profile must belong to the same application assurance group or partition.

a Associate an AA transit IP policy with the service object:

i Click on the Select button in the Transit IP Policy panel. The Select Transit IP Policy form opens.

ii Choose a transit IP policy and click on the OK button.

b Associate an AA transit prefix policy with the service object:

i Click on the Select button in the Transit Prefix Policy panel. The Select Transit Prefix Policy form opens.

ii Choose a transit IP policy and click on the OK button.

14 To configure custom object attributes for AA reporting to the 5670 RAM, perform the following steps:

i Click on the 5670 RAM Parameters tab.

ii Click on the Reporting tab.

iii Click on the Create button. The AA Reporting (Create) form opens.

iv Configure the parameters:

- Customer Name
- Subscriber Class
- Total Bandwidth Upstream (Kbps)
- Class of Service 1 Bandwidth Upstream (Kbps)
- Class of Service 2 Bandwidth Upstream (Kbps)
- Class of Service 3 Bandwidth Upstream (Kbps)
- Class of Service 4 Bandwidth Upstream (Kbps)
- Subscriber Name
- Subscriber Type
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)

v Click on the OK button. The AA Reporting (Create) form closes and the reporting object is displayed in the list.

vi Click on the General tab.

15 Perform one of the following to specify a transport tunnel for the Return SDP binding, if required.



Note — You can create a return tunnel only between sites that are within the same service. If the sites are not in the same service, the Return tab does not appear.

a Let the 5620 SAM configure the transport tunnel automatically.

i Click on the Return tab.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Configure the Profile Name or the Return Tunnel Auto-Selection Transport Preference parameter.

b Configure the transport tunnel manually.

i Click on the Return tab.

ii Click on the Select button in the Return Tunnel panel. The Select Return Tunnel - Spoke SDP Binding form opens.

iii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Return Tunnel - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the service Tunnel ID, Name, and Underlying Transport displayed in the Tunnel panel.

16 Associate a MEP to the spoke SDP binding, if required.

i Click on the MEPs tab.

ii Click on the Create button. The MEP (Create) form opens with the General tab displayed.

iii Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

iv Choose an entry and click on the OK button. The Select Maintenance Entity Group form closes.

v Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Propagation
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)
- CCM Padding Packet Size (Bytes)



Note — The CCM Padding Packet Size (Bytes) parameter cannot be configured when the CCM interval parameter is set to 10 ms or 100 ms.

17 If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab. Otherwise, go to step 21.

18 Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

19 Click on the AIS tab.

20 Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

21 Click on the OK button. A dialog box appears.

22 Click on the OK button. The MEP (Create) form closes.

23 Click on the OK button. The Spoke SDP Binding (Create) form closes and a dialog box appears.

24 Click on the OK button.

Procedure 71-57 To create an L2 SDP spoke termination on a VPRN service

Ensure that a service and site have been created in the VPRN. To terminate an L2 service on a VPRN SDP spoke, you must identify the VC and an interface belonging to the VC. The interface must not have an associated port.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN and click on the Properties button. The VPRN Service (Edit) form opens.

4 On the navigation tree, click on the site to which you need to create an L2 SDP spoke termination; expand the entries for that site.

5 Right-click on Spoke SDP Bindings and choose Create Spoke SDP Binding. The Spoke SDP Binding (Create) form opens with the General tab displayed.

6 Click on the Select button in the Source Interface panel to select an interface with no port assigned.

If you are creating this spoke SDP binding for use with an IP mirror interface, select the required IP mirror interface as the source interface.

7 Click on the OK button. The Select Interface - Spoke SDP Bindings form closes and the Spoke SDP Bindings (Create) form reappears with the interface information displayed.

8 Specify a destination node for the spoke SDP binding by performing one of the following tasks.

a If the destination node is a managed node, choose of managed nodes.

i Click on the Select button in the Tunnel Termination Site panel. The Select Destination Network Element - Spoke SDP Binding form opens.

ii Choose a destination node and click on the OK button. The Select Destination Network Element - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the tunnel termination site (the destination node) identifier displayed.

b If the destination node is an unmanaged node, specify the system ID for the Tunnel Termination Site parameter.

c If you are configuring IP mirroring, select a mirror source site as the tunnel termination site.

9 Configure the parameters:

- VC ID
- Auto-Assign ID
- VC Type
- Enable Ingress FlowSpec IPv4
- Enable Ingress FlowSpec IPv6

These parameters appear only when a source interface is assigned to the spoke SDP binding.

10 Configure the parameters in the Hash Label panel:

- Enable Hash Label
- Enable Signal Capability

The Enable Hash Label and Enable Signal Capability parameters can only be configured for spoke-SDP bindings that are access interface terminated.

11 Perform one of the following to specify a transport tunnel for the spoke SDP binding.

a Let the 5620 SAM configure the transport tunnel automatically.

i Enable the Auto-Select Transport Tunnel parameter.

ii Configure the Profile Name or the Tunnel Auto-Selection Transport Preference parameter.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens.

ii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier.

12 Choose an Application Profile for the spoke SDP binding.

i Click on the Select button beside the Application Profile parameter. The Application Profile String: - Spoke SDP Binding form opens.

ii Configure the filter criteria. A list of Application Profiles appears.

iii Choose an application profile and click on the OK button. The Application Profile String: - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form opens.



Note — The Application Profile String: - Spoke SDP Binding - VPRN service form displays only local profiles on the NE.

13 Choose one of the following AA transit policy types, if required.



Note 1 — You can only associate one AA transit policy type with a service object.

Note 2 — You can bind a transit policy to only one L3 access interface or spoke SDP binding per node.

Note 3 — The transit policy and the application profile must belong to the same application assurance group or partition.

a Associate an AA transit IP policy with the service object:

i Click on the Select button in the Transit IP Policy panel. The Select Transit IP Policy form opens.

ii Choose a transit IP policy and click on the OK button.

b Associate an AA transit prefix policy with the service object:

i Click on the Select button in the Transit Prefix Policy panel. The Select Transit Prefix Policy form opens.

ii Choose a transit IP policy and click on the OK button.

14 Click on the QoS tab.

15 Configure the required parameters in the Forwarding Plane Redirect panel:

i Click on the Network Policy Select button to assign a policy to the Spoke SDP Binding. The Select Network Policy form opens.

ii Choose a policy and click on the OK button. The Network Policy form closes and the Spoke SDP Binding (Create) form refreshes with the Network Policy information displayed.

iii Click on the Ingress Queue Group Template Policy Select button to assign a policy to the Spoke SDP Binding. The Select Ingress Queue Group Template Policy form opens.

iv Choose a policy and click on the OK button. The Ingress Queue Group Template Policy form closes and the Spoke SDP Binding (Create) form refreshes with the Ingress Queue Group Template Policy information displayed.

v Configure the Instance ID parameter.

16 Configure the required parameters in the Port Redirect panel:

i Click on the Network Policy Select button to assign a policy to the Spoke SDP Binding. The Select Network Policy form opens.

ii Choose a policy and click on the OK button. The Network Policy form closes and the Spoke SDP Binding (Create) form refreshes with the Network Policy information displayed.

iii Click on the Egress Queue Group Template Policy Select button to assign a policy to the Spoke SDP Binding. The Select Egress Queue Group Template Policy form opens.

iv Choose a policy and click on the OK button. The Egress Queue Group Template Policy form closes and the Spoke SDP Binding (Create) form refreshes with the Egress Queue Group Template Policy information displayed.

v Configure the Instance ID parameter.

17 Click on the States tab.

18 Configure the Administrative State parameter.

19 Assign ingress and egress ACL filters to the spoke SDP binding, if required.

i Click on the ACL tab.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - Spoke SDP Binding form opens.

iii Choose an ingress ACL filter. If you are configuring IP mirroring, you can optionally select an ingress IP filter. This is a packet mirroring option which specifies that packets matching the IP filter are mirrored to the mirror destination. Click on the OK button. The Select Ingress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form reappears with the ingress ACL filter information displayed.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - Spoke SDP Binding form opens.

v Choose an egress ACL filter and click on the OK button. The Select Egress Filter - Spoke SDP Binding form closes and the L3 Access Interface (Edit) form reappears with the egress ACL filter information displayed.

20 If you are configuring IP mirroring, go to step 22.

21 Assign an accounting policy to the spoke SDP binding, if required.

i Click on the Accounting tab.

ii Configure the Collect Accounting Statistics parameter.

iii Click on the Select button to choose an accounting policy. The Select Accounting Policy - Spoke SDP Binding form opens.

iv Choose an accounting policy and click on the OK button. The Select Accounting Policy - Spoke SDP Binding form closes and the L3 Access Interface (Edit) form reappears with the accounting policy information displayed.

22 Click on the OK button. The Spoke SDP Binding (Create) form closes and a dialog box appears.

23 Click on the OK button. The VPRN Service (Edit) form reappears with the new information displayed in the service navigation tree.

Procedure 71-58 To configure an MPLS-TP static pseudowire on a VPRN spoke SDP binding

Perform this procedure to create an MPLS-TP static pseudowire on the spoke SDP binding. An MPLS-TP service tunnel must be used in the SDP binding, and the Control Word parameter for pseudowire OAM must be set to Preferred. See Procedure 71-57.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Select a VPRN and click on the Properties button. The VPRN Service (Edit) form opens.

4 On the navigation tree, expand the site on which you want to configure the spoke SDP binding, and expand the Spoke SDP Bindings icon.

5 Click on the SDP binding on which you want to configure the MPLS-TP static pseudowire. The Spoke SDP Binding (Edit) form opens with the General tab displayed.

6 Click on the Control Channel tab.

7 Configure the parameters:

- Status
- Refresh Timer (seconds)
- Request Timer (seconds)

8 Click on the MPLS-TP PW tab.

9 Click on the Create button. The PW Path ID (Create) form opens.

10 Configure the Path AGI parameter.

11 Configure the parameters in the Source Attachment Individual Identifier panel:

- SAII Global ID
- SAII Node ID
- SAII AC ID

12 Configure the parameters in the Target Attachment Individual Identifier panel:

- TAII Global ID
- TAII Node ID
- TAII AC ID

13 Click on the OK button. The PW Path ID (Create) form closes.

14 Click on the OK button. The Spoke SDP Binding (Edit) form closes.

15 Close the VPRN Service (Edit) form.

16 Close the Manage Services form.

Procedure 71-59 To configure a subscriber interface on a VPRN

The 7450 ESS in mixed mode, 7710 SR and 7750 SR support the configuration of a subscriber interface in a VPRN.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPRN and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, navigate to the Subscriber Interfaces object. Perform one of the following:

a To create a subscriber interface, right-click on the Subscriber Interfaces object and choose Create VPRN Subscriber Interface from the menu. The VPRN Subscriber Interface (Create) form opens.

b To modify a subscriber interface, right-click on the subscriber interface object and choose Properties from the menu. The VPRN Subscriber Interface (Edit) form opens.

5 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- Default Primary DNS Server Address
- Default Secondary DNS Server Address
- Allow Unmatched Subnets
- Tunnel Fault Notification

The Tunnel Fault Notification parameter is configurable on interfaces where the device has ports configured in access or hybrid mode with QinQ encapsulation.

If you are configuring a tunnel facility MEP, Tunnel Fault Notification must be set to Accept, in order to receive the fault notification from the tunnel facility MEP.



Note 1 — The Name value for a subscriber interface must be unique in the context on the VPRN Service Site. That is, there cannot be another L3 access interface, subscriber interface, or group interface with the same name on the same VPRN site.

Note 2 — You must configure the Default Primary DNS Server Address parameter before you can configure the Default Secondary DNS Server Address parameter.

6 Configure IPv6 forwarding on the subscriber interface, if required.

i Configure the IPv6 Allowed parameter.

ii Configure the parameters.

- Admin Link Local Address
- IPv6 Delegated Prefix Length
- IPv6 Allow Unmatching Prefixes
- Default Primary IPv6 DNS Server Address
- Default Secondary IPv6 DNS Server Address

You must remove the check mark from the Default check box to access the Default Primary IPv6 DNS Server Address and Default Secondary IPv6 DNS Server Address parameters.

iii Click on the IPv6 Subscriber Prefixes tab.

iv Choose a subscriber prefix and click on the Properties button, or click on the Create button to create a new subscriber prefix.

v In the Subscriber Prefix [Edit|Create] form, configure the parameters:

- Address ID
- IP Address
- Prefix Length
- WAN Host
- Prefix Delegation

7 Configure the Interface Class parameters, if required.

i Configure the Class parameter.

ii If you selected a value of Unnumbered for the Class parameter, configure the Unnumbered Type parameter.

iii Configure the Interface Name parameter or the IP Address parameter.

8 Configure the DHCP Server Synchronization parameters, if required:

- Delayed Up Period
- Delay on Init Only

9 Perform one of the following:

a Create a subscriber interface for a wholesale and retail VPRN.

When you configure the routing instance for the VPRN, you can set the Type parameter to Subscriber Split Horizon to enable the forwarding service and forwarding subscriber information. The subscriber split horizon VPRN controls the flow of traffic for wholesale subscriber applications. See Procedure 71-1 for more information on how to configure this parameter.



Note — You cannot create a group interface under a forwarding subscriber interface.

Go to step 10.

b Create a subscriber interface for a traditional VPRN. Go to step 12.

10 Assign a forwarding service to the subscriber interface if you are configuring a wholesale and retail configuration for the VPRN.

i Click on the Select button in the Forwarding Service panel to choose a service. The Select Forwarding Service - VPRN Subscriber Interface form opens.

ii Choose a service and click on the OK button. The Select Forwarding Service - VPRN Subscriber Interface form closes, and the VPRN Subscriber Interface (Create) form reappears with the service information displayed.

iii Configure the Private Retail Subnet parameter that appears after you have assigned a forwarding service.

11 Assign a forwarding subscriber interface to the VPRN subscriber interface.

i Click on the Select button in the Forwarding Subscriber Interface panel to choose a subscriber. The Select Forwarding Subscriber Interface - VPRN Subscriber Interface form opens.

ii Choose a subscriber and click on the OK button. The Select Forwarding Subscriber Interface - VPRN Subscriber Interface form closes, and the VPRN Subscriber Interface (Create) form reappears with the subscriber information displayed.

12 Create IP addresses for the subscriber interface that are inherited by the SAPs in the group interfaces that are child objects of the subscriber interface.

i Click on the Addresses tab.

ii Click on the Create button. The IP Address (Create) form opens.

iii Configure the parameters:

- Address ID
- IP Address
- Prefix Length
- Populate Host Routes
- Track SRRP Instance
- Hold Up Time (milliseconds)
- Gateway IP Address
- Broadcast Address Format

iv Click on the OK button. The IP Address (Create) form closes, and a dialog box appears.

v Click on the OK button. The Subscriber Interface (Create) form reappears with the assigned IP addresses displayed.

vi Repeat steps ii to v for each additional IP address that you need to create.

13 Configure IPv4 DHCP for the interface, if required.

i Click on the DHCP tab.

ii If you specified a forwarding service in step 10, the General tab is configurable. Configure the parameters that define the forwarding service information. Otherwise go to step vii.

- Enable DHCP Relay
- Description
- Lease Populate

iii If you specified a forwarding service in step 10 and depending on the type and release of the device that you are configuring, the Subscriber Authentication Policy panel is present. Choose a Subscriber Authentication policy, if required. Otherwise, go to step vii.

iv Click on the Select button in the Subscriber Authentication Policy panel to choose a subscriber authentication policy. The Select Subscriber Authentication Policy - SubItfDhcpRelayCfg form opens.

v Configure the filter criteria. A list of available policies appears.

vi Choose a policy and click on the OK button. The Select Subscriber Authentication Policy - SubItfDhcpRelayCfg form closes, and the VPRN Subscriber Interface (Create) form refreshes with the subscriber authentication policy name.

vii Configure the parameters:

- IP Address
- Use as source

viii Click on the Server tab.

ix Configure the parameters.

- Server 1 through Server 8
- Administrative State
- Emulated Server IP Address
- Lease Time
- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time Override

The Number of Days, Number of Hours, Number of Minutes, Number of Seconds, and Lease Time Override parameters are configurable only when the Lease Time parameter is set to Specified Time Period.

x Click on the Client Applications tab.

xi Configure the Client Applications parameter. You can enable either or both of the PPPoE or DHCP choices.

14 Configure PPPoE for the interface, if required.



Note — PPPoE is only configurable on a VPRN subscriber interface if the interface is a retailer interface.

i Click on the PPPoE tab.

ii Configure the parameters:

- Description
- Session Limit

15 Configure the ARP host for the interface, if required.



Note — The ARP host is only configurable on a VPRN subscriber interface when the interface is a retailer interface.

i Click on the ARP Host Configuration tab.

ii Configure the parameters:

- Administrative State
- ARP Host Limit

16 Click on the OK button. The VPRN Subscriber Interface (Create) form closes, and a dialog box appears.

17 Click on the OK button. The VPRN Service (Edit) form reappears with the new subscriber interface displayed in the service navigation tree.

18 Click on the OK button. A dialog box appears.

19 Click on the Yes button. The VPRN Service (Edit) form closes, and the Manage Services form reappears.

20 Close the Manage Services form.

Procedure 71-60 To configure a group interface on a VPRN

The 7450 ESS in mixed mode, 7710 SR and 7750 SR support the configuration of a group interface in a VPRN.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, navigate to the site and subscriber interface on which you need to configure a group interface. Perform one of the following:

a To create a group interface, right-click on the subscriber interface and choose Create VPRN Group Interface from the menu. The VPRN Group Interface (Create) form opens.

b To modify a group interface, right-click on the group interface object and choose Properties from the menu. The VPRN Group Interface (Edit) form opens.

5 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- MAC Address
- Trusted
- LNS
- Specific Type
- Enable WPP
- IPv6 Allowed
- IPv6 IPoE Bridged Mode Enabled
- QoS Route Lookup IPv4
- QoS Route Lookup IPv6
- Configured IP MTU



Note — The LNS parameter defines the type of group interface (regular or LNS). This parameter is set at creation time and cannot be modified. Regular group interfaces cannot configure LNS attributes and an LNS group interface does not allow PPPoE configuration or SAPs.

6 If you enabled the IPv6 Allowed parameter in step 5, configure IPv6 router advertisement and DHCPv6 on the group interface.

i Click on the IPv6 Advertisement tab and configure the parameters:

- Administrative State
- Current Hop Limit
- Managed Address Config
- Max Interval (seconds)
- Min Interval (seconds)
- Link MTU
- Other Stateful Config
- Reachable Time (milliseconds)
- Retransmit Time (milliseconds)
- Router Lifetime (seconds)
- Autonomous Address Configuration
- Preferred Life Time
- Lifetime (seconds)

ii Click on the DHCPv6 tab.

iii Click on the Select button and select a local user database from the Select Local User Database form.

iv Click on the Proxy Server tab and configure the parameters:

- Administrative State
- Renew Timer
- Rebind Timer
- Valid Life Time
- Preferred Life Time
- Client Applications
- Server ID Type
- ID Type
- Value



Note — The ID Type and Value parameters are configurable only if the Server ID Type parameter is set to Enterprise.

v Click on the Relay tab and configure the parameters:

- Administrative State
- Description
- Remote ID
- Client Applications
- Link Address

vi Configure the Server 1 through Server 8 parameters.

vii Configure the interface name for each DHCPv6 server by clicking on the Select button in the Zone Index panel. The Select Zone Index - GrplfDhcpv6RelayCfg form opens with a list of local L3 access interfaces.

viii Choose an interface and click on the OK button. The Select Zone Index - GrplfDhcpv6RelayCfg form closes and the VPRN Group Interface form refreshes with the interface name.



Note — If you have entered a Unicast address, then the Interface Name parameter is not required.

7 If you enabled the Enable WPP parameter in step 5, configure WPP on the group interface.

i Click on the WPP tab.

ii Configure the Administrative State parameter.

iii Click on the Select button in the WPP Site panel and choose a WPP site from the Select WPP Site form.

iv Configure the Portal Name parameter.

v Click on the Select button beside the Initial Subscriber Profile parameter and choose a subscriber profile from the Select Subscriber Profile form.

vi Click on the Select button beside the Initial SLA Profile parameter and choose an SLA profile from the Select SLA Profile form.

vii Click on the Select button beside the Initial Application Profile parameter and choose an application profile from the Select Application Profile form.

viii Configure the Restore Default Profile On Disconnection parameter.

8 Click on the Anti-Spoofing tab.

9 Configure the ARP Populate parameter.

10 Click on the Subscriber Management tab.

11 Configure the parameters:

- SHCV Enabled
- SHCV Interval (minutes)
- SHCV Source
- SHCV Action
- SHCV Retry Timeout (seconds)
- SHCV Retry Count
- SHCV Family

12 As required, configure ICMP for the group interface.

i Click on the ICMP tab.

ii Configure the parameters:

- Mask Reply
- Redirects
- Unreachables
- TTL Expired
- Number of Redirects
- Redirects Time (seconds)
- Number of Unreachables
- Unreachables Time (seconds)
- Number of TTL Expired
- TTL Expired Time (seconds)

13 As required, configure ARP for the group interface.

i Click on the ARP tab. The General tab is displayed.

ii Configure the Timeout (seconds) parameter.

iii Click on the Proxy ARP tab.

iv Configure the parameters:

- Remote Proxy ARP
- Enable Local Proxy ARP
- Proxy ARP Policy 1 through Proxy ARP Policy 5

14 As required, configure IPv4 DHCP relay for the group interface.

i Click on the DHCP tab. The DHCP form opens with the General tab displayed.

ii Configure the parameters:

- Enable DHCP Relay
- Description
- Match Circuit ID
- Trusted
- Lease Populate
- L2 Header
- Anti-Spoof MAC Address
- Action
- Circuit ID
- Remote ID
- Remote ID String
- Vendor Specific Options
- Vendor String
- IP address (GI address)
- Use as source
- Relay Unicast Message

When the Relay Unicast Message parameter is set to Renew or Release Update Source IP, the GI address parameter can be configured as any local configured address in the same routing instance as the GI address for the DHCP relayed messages. If the Relay Unicast Message parameter is set to None, the GI address is restricted to the IP address configured on the subscriber interface.

iii Depending on the type and release of device that you are configuring, the Subscriber Authentication Policy panel is present. Choose a Subscriber Authentication policy, if required. Otherwise, go to step xiii.

iv Click on the Select button in the Subscriber Authentication panel to choose a subscriber authentication policy. The Select Subscriber Authentication Policy - GrpItfDhcpRelayCfg form opens.

v Configure the filter criteria. A list of available policies appears.

vi Choose a policy and click on the OK button. The Select Subscriber Authentication Policy - GrpItfDhcpRelayCfg form closes, and the VPRN Group Interface (Create) form reappears with the policy name information displayed.

vii Click on the Select button in the Local User Database panel to choose a local user database. The Select localUserDbPointer - GrpItfDhcpRelayCfg form opens.

viii Configure the filter criteria. A list of available databases appears.

ix Choose a database and click on the OK button. The Select localUserDbPointer - GrpItfDhcpRelayCfg form closes, and the VPRN Group Interface (Create) form reappears with the database name information displayed.

x Click on the Select button in the DHCP Filter panel to choose a filter policy to bind with the group interface. The Select dhcpFilterPointer - GrpItfDhcpRelayCfg form opens.

xi Configure the filter criteria, and click on the Search button. A list of available filter policies appears.

xii Choose a filter policy and click on the OK button. The Select dhcpFilterPointer - GrpItfDhcpRelayCfg form closes, and the VPRN Group Interface (Create) form reappears with the filter policy information displayed.

xiii Click on the Server tab.

xiv Configure the parameters:

- Server 1 to Server 8
- Administrative State
- Emulated Server IP Address
- Lease Time
- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time Override

The Number of Days, Number of Hours, Number of Minutes, Number of Seconds, and Lease Time Override parameters are configurable only when the Lease Time parameter is set to Specified Time Period.

xv Click on the Client Applications tab and configure the Client Applications parameter.

15 Click on the Default Hosts tab to create a default host where the associated DHCP filter policy is configured with the Bypass Host creation action. See Procedure 44-7 for more information about DHCP filter creation. See step 14 x in this procedure for more information about how to bind a DHCP filter with the group interface.

i Click on the Create button. The Default Host (Create) form opens.

ii Click on the Select button in the Default Host Configuration panel to choose the Default Host IP Address parameter value for the DHCP filter policy to associate with the subscriber interface SAP. The Select Default Host Configuration form opens.

iii Configure the filter criteria, and click on the Search button. A list of available DHCP filter policies appears.

iv Choose a DHCP filter policy and click on the OK button. The Select Default Host Configuration form closes, and the Default Host (Create) form reappears with the IP address for the selected DHCP filter policy displayed.

v Configure the Next Hop IP Address parameter.

vi Click on the Apply button. The Default Host (Create) form closes and the default host is added to the Default Hosts list.

16 Configure PPP for the group interface, if required.

i Click on the PPP tab.

ii Configure the Description and Administrative State parameters in the PPPoE panel.

iii Click on the Select button beside the Policy field in the PPPoE panel and choose a PPPoE policy from the Select Policy form.

iv Click on the Select button beside the Local User DB field in the PPPoE panel and choose a PPPoE Local User DB from the The Select Local User DB form.

v Configure the remaining parameters in the PPPoE panel:

- Session Limit
- Session Limit per SAP
- Anti-Spoofing
- CCAG Use Original SAP
- Vendor Specific Option String

vi Configure the Description and Administrative State parameters in the PPP panel.

vii Click on the Select button beside the Policy field in the PPP panel and choose a PPP policy from the Select Policy form.

viii Click on the Select button beside the Local User DB field in the PPP panel and choose a PPP Local User DB from the The Select Local User DB form.

ix Configure the Session Limit parameter in the PPP panel

17 Configure IPoE linkage for the group interface, if required.

i Click on the IPoE Linkage tab.

ii Configure the parameters:

- Administrative State
- Sharing Circuit-ID
- Unsolicited Router Advertisements

18 Configure the ARP host for the group interface, if required.

i Click on the ARP Host Configuration tab.

ii Configure the parameters:

- Administrative State
- ARP Host Limit
- Minimum Authentication Interval (minutes)
- SAP ARP Host Limit

19 Configure local address assignment for the group interface, if required.

i Click on the Local Address Assignment tab.

ii Configure the parameters:

- Administrative State
- Default Pool Name
- Secondary Pool Name

iii On the IPv4 Options panel, configure the PPP-v4 parameter and select a local DHCP server, if required.

iv On the IPv6 Options panel, configure the IPoE WAN and PPP SLAAC parameters and select a local DHCPv6 server, if required.

20 If you set the LNS parameter to TRUE in step 5, configure LNS for the group interface.



Note — After you create an LNS group interface, you must configure the L2TP tunnel group profile or tunnel profile to terminate sessions for the LNS group interface that you just created; see Procedure 23-34. You can also configure the termination of sessions on a group interface using a RADIUS server.

i Click on the LNS tab.

ii Configure the Description parameter.

iii Click on the Select button in the Default Subscriber Profile panel. The Select Default Subscriber Profile (Terminate LNS PPP Sessions) form opens with a list of available profiles.

iv Choose a subscriber profile and click on the OK button. The Select Default Subscriber Profile (Terminate LNS PPP Sessions) form closes and the VPRN Group Interface (Create) form reappears with the Subscriber Profile displayed.

v Click on the Select button in the Default SLA Profile panel. The Select Default SLA Profile (Terminate LNS PPP Sessions) form opens with a list of available SLA profiles.

vi Choose an SLA profile and click on the OK button. The Select Default SLA Profile (Terminate LNS PPP Sessions) form closes and the VPRN Group Interface (Create) form reappears with the SLA Profile displayed.

vii Click on the Select button in the Subscriber Identification Policy panel. The Select Subscriber Identification Policy (Terminate LNS PPP Sessions) form opens with a list of available subscriber identification policies.

viii Choose a subscriber identification policy and click on the OK button. The Select Subscriber Identification Policy (Terminate LNS PPP Sessions) form closes and the VPRN Group Interface (Create) form reappears with the subscriber identification policy displayed.

ix Click on the Select button in the Default Application Profile panel. The Select Default Application Profile (Terminate LNS PPP Sessions) form opens with a list of available default application profiles.

x Choose a default application profile and click on the OK button. The Select Default Application Profile (Terminate LNS PPP Sessions) form closes and the VPRN Group Interface (Create) form reappears with the default application profile displayed.

xi Configure the Default Subscriber Identification String parameter.

21 Click on the Service Access Points tab to configure SAPs for the group interface.

22 Click on the Create button. The VPRN Service Access Point (Create) form opens with the General tab displayed.

23 Configure the parameters:

- Name
- Description
- Administrative State
- Calling Station ID

24 Associate a host lockout policy with the group interface, if required. Click on the Select button in the Host Lockout panel to select a policy.

25 Click on the Port tab.

26 Click on the Select button to choose a port for the L3 access interface. The Select Terminating Port - VPRN L3 Access Interface form opens.



Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

27 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - VPRN L3 Access Interface form closes, and the VPRN L3 Access Interface (Create) form displays the port information.

28 Configure the parameters:

- Auto-Assign ID
- Outer Encapsulation Value
- Inner Encapsulation Value
- Outer Encapsulation Value (VPI)
- Inner Encapsulation Value (VCI)
- SAP Description
- SAP Administrative State

The Auto-Assign ID parameter is configurable if the port uses dot1q encapsulation. When the parameter is enabled, the 5620 SAM automatically configures the Outer Encapsulation Value parameter using the lowest unassigned value.



Note — You can set the Auto-Assign ID parameter to be the default parameter for dot1q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter on the User Preferences form. Choose Application→ User Preferences from the main menu.

The Inner Encapsulation Value is configurable only when the port is an Ethernet or frame relay port with QinQ encapsulation.

The Outer Encapsulation Value (VPI) and Inner Encapsulation Value (VCI) parameters are configurable only for ATM ports.

29 Assign ingress and egress QoS policies to the SAP, if required.



Note — Items such as policies, schedulers, and filters can be applied later to multiple service components at once. Choose and right-click the components in the service navigation tree, choose Properties, and configure the parameters on the appropriate tab.

i Click on the QoS tab.

ii Configure the parameters:

- Ingress Match QinQ Dot1P
- Egress Mark QinQ Top Bits Only
- Use SAP ID as Subscriber ID

The Ingress Match QinQ Dot1P and Egress Mark QinQ Top Bits Only parameters are configurable only when the encapsulation type of the port is BCP dot1q, dot1q, or QinQ.

iii Click on the Select button in the Ingress Policy panel to choose an ingress QoS policy. The Select Ingress Policy - VPRN Service Access Point form opens.

iv Configure the filter criteria and click on the Search button. A list of available ingress policies appear.

v Choose an ingress QoS policy and click on the OK button. The Select Ingress Policy - VPRN Service Access Point form closes, and the VPRN Service Access Point (Create) form reappears with the ingress QoS policy information displayed.



Note — If you select an ingress policy which has a forwarding class mapped to an ingress queue group, you must ensure that the port you selected in step 27 has the access ingress queue group with the same name created on it.

See Procedure 16-1 for more information about how to configure Ethernet ports. See chapter 42 for more information about queue group template policies.

vi Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - VPRN Service Access Point form opens.

vii Configure the filter criteria and click on the Search button. A list of available egress policies is displayed.

viii Choose an egress QoS policy and click on the OK button. The Select Egress Policy - VPRN Service Access Point form closes, and the VPRN Service Access Point (Create) form reappears with the egress QoS policy information displayed.



Note — If you select an egress policy which has a forwarding class mapped to an egress queue group, you must ensure that the port you selected in step 27 has the access egress queue group with the same name created on it.

See Procedure 16-1 for more information about how to configure Ethernet ports. See chapter 42 for more information about queue group template policies.

30 Click on the Schedulers tab to configure scheduling; otherwise, go to step 32.



Note — The Schedulers tab is configurable only if a port is assigned to the SAP earlier in the procedure.

31 Perform one of the following.

a Specify that an aggregation scheduler policy is not applied to the SAP.

i Set the Aggregation parameter to off.



Note — The Aggregation parameter is not configurable if the port you selected in step 27 is an HSMDA port.

ii Configure the parameters:

- Aggregate Rate Limit (kbps)
- Frame-Based Accounting



Note 1 — The Aggregate Rate Limit (kbps) and Frame-Based Accounting parameters are configurable only when there is no scheduler specified in the Egress Scheduler panel.

Note 2 — The Frame-Based Accounting parameter is not configurable if the port you selected in step 27 is an HSMDA port.

Note 3 — You cannot specify an egress scheduler when the Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

iii Click on the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - VPRN Service Access Point form opens.

iv Choose an ingress scheduler and click on the OK button. The Select Ingress Scheduler - VPRN Service Access Point form closes, and the VPRN Service Access Point (Create) form refreshes with the ingress scheduler information displayed.

v Click on the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Ingress Policer Control Policy form opens.

vi Choose a policer control policy and click on the OK button. The Select Ingress Policer Control Policy form closes and the VPRN Service Access Point (Create) form reappears with the ingress policer control policy information displayed.

vii If the port you selected in step 27 is an HSMDA port, go to step 32.

viii Click on the Select button in the Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - VPRN Service Access Point form opens.

ix Choose an egress scheduler and click on the OK button. The Select Egress Scheduler - VPRN Service Access Point form closes, and the VPRN Service Access Point (Create) form refreshes with the egress scheduler information displayed.

x Click on the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Egress Policer Control Policy form opens.

xi Choose a policer control policy and click on the OK button. The Select Egress Policer Control Policy form closes and the VPRN Service Access Point (Create) form reappears with the egress policer control policy information displayed.

xii Go to step 32.

b Specify that an aggregation scheduler policy is applied to the SAP.

i Set the Aggregation parameter to on.



Note — You cannot specify an access scheduler policy if the port you selected in step 27 is an HSMDA port. Go to step 32.

ii Configure the Frame-Based Accounting parameter.

iii Click on the Select button in the Aggregation Scheduler panel to choose an aggregation scheduler. The Select Aggregation Scheduler - VPRN Service Access Point form opens.

iv Choose an aggregation scheduler and click on the OK button. The Select Aggregation Scheduler - VPRN Service Access Point form closes, and the VPRN Service Access Point (Create) form refreshes with the aggregation scheduler information displayed.

32 Assign ingress and egress ACL filters to the SAP, if required.

i Click on the ACL tab.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter from the Select Ingress Filter - VPRN Service Access Point form.

iii Click on the Select button in the Egress Filter panel to choose an egress ACL filter from the Select Egress Filter - VPRN Service Access Point form.

33 Click on the Accounting tab to assign an accounting policy to the SAP.

i Configure the Collect Accounting Statistics parameter.

ii Click on the Select button to choose an accounting policy. The Select Accounting Policy - VPRN Service Access Point form opens.

iii Choose an accounting policy and click on the OK button. The Select Accounting Policy - VPRN Service Access Point form closes, and the VPRN Service Access Point (Create) form reappears with the accounting policy information displayed.

34 Click on the Anti-Spoofing tab to configure anti-spoofing for the SAP.

i Configure the Anti-Spoofing parameter.

To configure residential subscriber management for static hosts, the Anti-Spoofing parameter must be set to at least IP-address matching, or optionally, to IP- and MAC-address matching.

ii Click on the Static Hosts tab to add a static host to the SAP.

iii Click on the Static Hosts tab to configure a static subscriber host entry for each subscriber host that is not managed by DHCP.

iv Click on the Create button. The Access Interface Anti-Spoofing Static Host Display (Create) form opens.

v Configure the parameters:

- IP Address
- MAC Address
- Subscriber Identification

vi Configure residential subscriber management for the static host.

vii Click on the Select button in the Subscriber Profile panel to choose a subscriber profile for the static host, if required. The Select Subscriber Profile - AntiSpoofingStaticHosts form opens with the list of available subscriber profiles displayed. Otherwise, go to step 35.

viii Choose a subscriber profile and click on the OK button. The Select Subscriber Profile - AntiSpoofingStaticHosts form closes, and the subscriber profile name appears in the Subscriber Profile panel.

ix Click on the Select button in the SLA Profile panel to choose an SLA profile for the static host. The Select SLA Profile - AntiSpoofingStaticHosts form opens with the list of available SLA profiles displayed.

x Choose an SLA profile and click on the OK button. The Select SLA Profile - AntiSpoofingStaticHosts form closes, and the SLA profile name appears in the SLA Profile panel.

xi Click on the Select button in the Application Profile panel to choose an application profile for the static host. The Select Application Profile - AntiSpoofingStaticHosts form opens with the list of application profiles on the NE displayed.

xii Choose an application profile and click on the OK button. The Select Application Profile - AntiSpoofingStaticHosts form closes, and the application profile name appears in the Application Profile panel.

35 Click on the OK button. A dialog box appears.

36 Click on the OK button. The Access Interface Anti-Spoofing Static Host Display (Create) form closes.

37 Assign a DoS protection policy or DDoS protection policy to the SAP, if required.



Note — A default DoS protection policy is automatically assigned to the SAP.

i Click on the Security tab.

ii Click on the Select button in the NE DoS Protection panel and select a DoS protection policy from the Select NE DoS Protection form.

iii Click on the Select button next to the NE DDoS Protection field and select a DDoS protection policy from the Select NE DDoS Protection Policy form.

iv Configure the MAC Monitoring parameter.

38 Click on the Subscriber Management tab to configure residential subscriber management on the SAP. The IGMP Host Tracking tab is displayed.

i Click on the Select button to choose the import policy used to filter IGMP packets. The Select SapIgmpHostTracking form opens.

ii Configure the filter parameters and click on the Search button. A list of import policies appears.

iii Choose a policy and click on the OK button. The selected import policy name appears.

iv Configure the parameters:

- Expiry Time (seconds)
- Max Number of Groups
- Max Number of Sources per Group
- Disable Router Alert Check

v You can click on the Host Tracking Info tab to view a list of hosts that are being tracked on this service access point.

vi Click on the Profiles tab.

vii Configure the parameters:

- Admin Status
- Service Model
- Subscriber Limit
- Profiled Traffic only
- Non-Subscriber Traffic Identification
- Default Subscriber Identification Type
- Default Subscriber ID
- Default Intermediate Destination Id Type
- Default Intermediate Destination Id

viii Click on the Select button in the Default Subscriber Profile panel to choose a default subscriber profile for the SAP, if required. The Select Default Subscriber Profile form opens with the list of available subscriber profiles displayed.

ix Choose a subscriber profile and click on the OK button. The Select Default Subscriber Profile form closes, and the subscriber profile name appears in the Default Subscriber Profile panel.

x Click on the Select button in the Default SLA Profile panel to choose a Default SLA profile for the SAP, if required. The Select Default SLA Profile form opens with the list of available SLA profiles displayed.

xi Choose an SLA profile and click on the OK button. The Select Default SLA Profile form closes, and the SLA profile name appears in the Default SLA Profile panel.

xii Click on the Select button in the Subscriber Identification Policy panel to choose a subscriber identification policy for the SAP, if required. The Select Subscriber Identification Policy form opens with the list of available subscriber identification policies displayed.

xiii Choose a subscriber identification policy and click on the OK button. The Select Subscriber Identification Policy form closes, and the subscriber identification policy name appears in the Subscriber Identification Policy panel.

xiv Click on the Select button in the Default Application Profile panel to choose a default application profile for the SAP, if required. The Select Default Application Profile form opens with the list of application profiles on the NE displayed.

xv Choose an application profile and click on the OK button. The Select Default Application Profile form closes, and the application profile name appears in the Default Application Profile panel.

xvi Click on the Select button in the Non-Subscriber Traffic Subscriber Profile panel to choose a non-subscriber subscriber profile for the SAP, if required. The Select Non-Subscriber Traffic Subscriber Profile form opens with the list of available subscriber profiles displayed.

xvii Choose a subscriber profile and click on the OK button. The Select Non-Subscriber Traffic Subscriber Profile form closes, and the subscriber profile name appears in the Non-Subscriber Traffic Subscriber Profile panel.

xviii Click on the Select button in the Non-Subscriber Traffic SLA Profile panel to choose a Non-Subscriber Traffic SLA profile for the SAP, if required. The Select Non-Subscriber Traffic SLA Profile form opens with the list of available SLA profiles displayed.

xix Choose an SLA profile and click on the OK button. The Select Non-Subscriber Traffic SLA Profile form closes, and the SLA profile name appears in the Non-Subscriber Traffic SLA Profile panel.

xx Click on the Select button in the Non-Subscriber Traffic Application Profile panel to choose a non-subscriber traffic application profile for the SAP, if required. The Select Non-Subscriber Traffic Application Profile form opens with the list of application profiles on the NE displayed.

xxi Choose an application profile and click on the OK button. The Select Non-Subscriber Traffic Application Profile form closes, and the application profile name appears in the Non-Subscriber Traffic Application Profile panel.

xxii Click on the Subscriber Hosts tab to view active hosts for the subscriber instance, if required.

39 Configure ATM on the SAP, if required.

i Click on the ATM tab.

ii Configure the parameters:

- AAL5 Encapsulation
- ATM OAM Alarm Cell Handling
- Periodic ATM OAM Loopback

iii Click on the Select button in the Ingress ATM Policy panel to choose an ingress ATM policy. The Select Ingress ATM Policy - ATM Configuration form opens.

iv Choose an ingress ATM policy and click on the OK button. The Select Ingress ATM Policy - ATM Configuration form closes, and the VPRN Service Access Point (Create) form refreshes with the ingress ATM policy information displayed.

v Click on the Select button in the Egress ATM Policy panel to choose an egress ATM policy. The Select Egress ATM Policy - ATM Configuration form opens.

vi Choose an egress ATM policy and click on the OK button. The Select Egress ATM Policy - ATM Configuration form closes, and the VPRN Service Access Point (Create) form refreshes with the egress ATM policy information displayed.

40 Click on the OK button. The VPRN Service Access Point (Create) form closes and a dialog box appears.

41 Click on the OK button. The VPRN Group Interface (Create) form refreshes to display the SAP.

42 To configure an additional SAP in the group interface, go to step 22.

43 Click on the SRRP tab.

44 Configure the parameters in the Routing panel:

- Enabled
- Hold Time (seconds)

45 Click on the Create button in the SRRP Instance panel. The SRRP Instance (Create) form opens with the General tab displayed.

46 Configure the parameters:

- SRRP ID
- Description
- Administrative State

47 Click on the Select button in the Operational Group panel. The Select Monitored Group Name - SRRP Instance form opens.

48 Choose a Monitored Group Name and click on the OK button. The Select Monitored Group Name - SRRP Instance form closes.

49 Configure the Priority Step parameter.

50 Click on the Behavior tab.

51 Configure the General parameters:

- Gateway MAC Address
- Keep Alive Interval
- Priority
- Preempt
- FIB Population Mode
- One Gratuitous ARP Per SAP

52 Click on the Select button in the Message Path panel. The Select Message Path Pointer - SRRP Instance form opens, displaying the SAPs available on the site.

53 Select the SAP you need to use for the in-band messaging between the sites and click on the OK button. The Select Message Path Pointer - SRRP Instance form closes.

54 Click on the Select button in the Policy Pointer 1 panel. The Select Policy Pointer 1 - SRRP Instance form opens.

55 Choose an entry and click on the OK button. The Select Policy Pointer 1 - SRRP Instance form closes.

56 Click on the Select button in the Policy Pointer 1 panel. The Select Policy Pointer 2 - SRRP Instance form opens.

57 Choose an entry and click on the OK button. The Select Policy Pointer 2 - SRRP Instance form closes.

58 Click on the OK button. The SRRP Instance (Create) form closes and a dialog box appears.

59 Click on the OK button.

60 Click on the OK button. The VPRN Group Interface (Create) form closes and a dialog box appears.

61 Click on the OK button. The VPRN Service (Edit) form refreshes to display the SAP below the group interface.

62 Click on the OK button. A dialog box appears.

63 Click on the Yes button. The VPRN Service (Edit) form closes.

64 Close the Manage Services form.

Procedure 71-61 To collect and view PPP ATM SAP statistics and information for a VPRN group interface

See "Statistics collection overview" in the *5620 SAM Statistics Management Guide* for general information about configuring and collecting statistics.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Choose VPRN Service (VPRN) from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of VPRN services appears.

4 Choose a service and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

5 On the navigation tree, click on a group interface. The VPRN Group Interface (Edit) form opens.

6 Click on the Statistics tab.

7 Choose PPP ATM SAP (Service Management) from the object drop-down list.

8 Click on the Collect button to collect the PPP ATM SAP statistics.

9 Choose a statistics record and click on the Properties button to view the record. The statistics record form opens.

10 View the statistics information.

11 Click on the Close button to close the statistics record form.

12 Repeat steps 9 to 11 for each statistics record that you need to view.

13 Close the VPRN Group Interface (Edit) form.

14 Close the VPRN Service (Edit) form.

15 Close the Manage Services form.

Procedure 71-62 To configure a WLAN GW for a VPRN group interface

Before you can configure a WLAN GW for a VPRN group interface, you must configure a VPRN group interface with the Specific Type parameter set to Soft GRE. See Procedure 71-60.

1 Choose Manage→Service→Services from the navigation tree view selector. The Manage Services form opens.

2 Choose VPRN Site (VPRN) from the Object drop-down list.

3 Click on the Search button. A list of VPRN sites is displayed.

4 Select a VPRN site with a VPRN group interface and click on the Properties button. The VPRN Site form opens with the general tab displayed.

For the purposes of WLAN GW configuration, you must choose a Soft GRE type VPRN group interface.

5 On the VPRN Site form navigation tree, expand the Subscriber Interfaces icon.

6 Expand a subscriber interface with a VPRN group interface.

7 Click on a VPRN group interface. The general tab is displayed.

8 Click on the WLAN GW tab.

9 Click on the Select button in the WLAN GW Group panel and choose a WLAN GW group form the Select WLAN GW Group form.

10 Click on the Select button in the Tunnel Router Instance panel and choose a tunnel router instance from the Select Tunnel Router Instance form.

11 Configure the WLAN Gateway Address parameter.

12 Click on the Select button in the Default Retail Service panel and choose a default retail IES service from the Select Default Retail Service form.

13 Configure the parameters:

- TCP Maximum Segment Size Adjustment
- Data Triggered UE Creation
- Mobility Detection Trigger
- Hold Time

14 Configure egress QoS, if required.

i In the Egress QoS panel, configure the parameters:

- Multi Client Only Shaping
- Shaping
- Hold Time
  Enabling the Infinite check box sets the Hold Time parameter to infinite.

ii Click on the Select button beside the QoS Policy field and choose an access egress policy from the Select QoS - Soft GRE Config form.

iii Click on the Select button beside the Scheduler Policy field and choose a scheduler policy from the Select Scheduler - Soft GRE Config form.

iv Configure the Aggregate Rate Limit parameter. Do not configure this parameter with a positive value if you specified a scheduler policy in step iii.

15 Click on the Select button beside the Authentication Policy field and choose an authentication policy from the Select ISA RADIUS Policies - Soft GRE Config form.

16 Configure an authentication hold time, if required:

i Enable the check box in the Authentication Hold Time panel.

ii Specify an authentication hold time in the Hours, Minutes, and Seconds fields.

17 Configure SAP parameters, as required.

i Click on the SAP Parameters tab.

ii Configure the Description parameter.

iii Click on the Select button beside the Subscriber Profile parameter and choose a subscriber profile from the Select Subscriber Profile form.

iv Click on the Select button beside the SLA Profile parameter and choose an SLA profile from the Select SLA Profile form.

v Click on the Select button beside the Application Profile parameter and choose an application profile from the Select Application Profile form.

vi Click on the Select button beside the Subscriber Identification Policy parameter and choose a subscriber identification policy from the Select Subscriber Identification Policy form.

vii Configure the Default ID Type parameter.

viii If the Default ID Type parameter was set to Use String, configure the Default ID String parameter.

18 Configure DHCP, as required.

i Click on the DHCP tab.

ii Configure the parameters:

- Administrative State
- L2 Aware IP Address
- IP Address Lease Time (Initial State)
  Remove the check mark from the Default check box and configure the Hours, Minutes, and Seconds parameters.
- IP Address Lease Time (Active State)
  Remove the check mark from the Default check box and configure the Hours, Minutes, and Seconds parameters.
- Primary DNS Server
- Secondary DNS Server
- Primary NBNS Server
- Secondary NBNS Server

iii Click on the Select button next to the NAT Policy field and choose a NAT policy from the Select NAT Policy form.

iv Click on the Select button next to the HTTP Redirect Policy field and choose an HTTP redirect policy from the Select HTTP Redirect Policy form.

19 Configure VLAN tag ranges, as required.

i Click on the VLAN Tag Ranges tab.

ii Click on the Create button. The VLAN Tag Range form opens.

iii Configure the parameters:

- Start VLAN Tag
- End VLAN Tag

iv Click on the Select button next to the Retail Service ID field and choose a retail service from the Select Retail Service form.

v Configure the Data Triggered User Equipment Creation parameter.

vi Click on the Select button next to the NAT Policy field and choose a NAT policy from the Select NAT Policy form.

vii Click on the Select button next to the HTTP Redirect Policy field and choose an HTTP redirect policy from the Select HTTP Redirect Policy form.

viii Click on the Select button next to the Authentication Policy field and choose an authentication policy from the Select Authentication Policy form.

ix Configure the Hold Time parameter. Remove the check mark from the Default check box and configure the Hours, Minutes, and Seconds parameters.

x Configure the Routing Instance parameter.

xi Click on the Select button in the RADIUS Proxy Cache panel and choose a RADIUS proxy cache server from the Select RADIUS Proxy Cache form.

xii Configure the MAC Address Format and Show Format parameters.

xiii Configure DHCP, as required.

xiv Click on the DHCP tab.

xv Configure the parameters:

- Administrative State
- L2 Aware IP Address
- IP Address Lease Time (Initial State)
  Remove the check mark from the Default check box and configure the Hours, Minutes, and Seconds parameters.
- IP Address Lease Time (Active State)
  Remove the check mark from the Default check box and configure the Hours, Minutes, and Seconds parameters.
- Primary DNS Server
- Secondary DNS Server
- Primary NBNS Server
- Secondary NBNS Server

xvi Click on the OK button. A dialog box appears.

xvii Click on the OK button. The VLAN Tag Ranges tab is updated with the new VLAN tag range displayed.

20 Click on the OK button. A dialog box appears.

21 Click on the OK button. The VPRN Site (Edit) form closes.

22 Close the Manage Services form.

Procedure 71-63 To add an IP mirror interface to a VPRN

Perform this procedure to configure an IP mirror interface in a VPRN service. This is a spoke terminated interface used to receive mirrored packets from a remote source.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site to which you need to add the IP mirror interface; expand the entries for that site.

5 Right-click on IP Mirror Interfaces and choose Create IP Mirror Interface. The IP Mirror Interface (Create) form opens.

6 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State



Note — The Name value for an IP mirror interface must be unique in VPRN site. There cannot be another L3 access interface, subscriber interface, or group interface with the same name on the VPRN site.

7 Click on the OK button. The IP Mirror Interface (Create) form closes and a dialog box appears.

8 Click on the OK button. The VPRN Service (Edit) form reappears with the IP mirror interface displayed in the service navigation tree.

9 Create a spoke SDP binding for the interface by performing steps 5 to 23 of Procedure 71-57.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The VPRN Service (Edit) form closes, and the Manage Services form reappears.

12 Close the Manage Services form.

Procedure 71-64 To add a TMS interface to a VPRN

The 7750 SR-7 and 7750 SR-12 devices support the configuration of a TMS interface in a VPRN.

The following conditions must be met before you can configure a TMS interface.

- You must have one VPRN configured. The TMS interface is configured on this on-ramp VPRN.
- Optionally, you can have two addition VPRNs configured, one for the management VPRN and one for the off-ramp VPRN.
- Each VPRN must be associated within the same site on the same node.
- The ISA-TMS daughter card must be installed.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears.

3 Choose a VPRN and click on the Properties button. The VPRN Service Subscriber (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site to which you need to add the TMS interface; expand the entries for that site.

5 Right-click on the TMS Interfaces icon and choose Create TMS Interface. The TMS Interface (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- IPv6 Allowed



Note — The Name value for a TMS interface must be unique in the context of the VPRN Service Site. That is, there cannot be another L3 access interface, subscriber interface, group interface or TMS interface with the same name on the same VPRN site.

7 Assign an off-ramp VPRN to the TMS interface

i Click on the Select button in the Off-Ramp VPRN panel and Choose a VPRN from the Select Off-Ramp VPRN - TMS Interface form.

ii Click on the OK button. The Select Off-Ramp VPRN - TMS Interface form closes, and the TMS Interface (Create) form reappears with the VPRN information displayed.

8 Assign a management VPRN to the TMS interface

i Click on the Select button in the Management VPRN panel and Choose a VPRN from the Select Management VPRN - TMS Interface form.

ii Click on the OK button. The Select Management VPRN - TMS Interface form closes, and the TMS Interface (Create) form reappears with the subscriber information displayed.

9 Associate an ISA-TMS daughter card with the TMS interface.



Note — An ISA-TMS card can only be assigned to one TMS interface.

i Click on the Select button in the TMS Info panel and select an ISA-TMS to associate with the TMS interface from the Select ISA-TMS - TMS Interface form.

ii Click on the OK button. The Select ISA-TMS - TMS Interface form closes, and the TMS Interface (Create) form reappears with the slot name for the daughter card displayed.

10 Configure the ISA-TMS Authentication parameter.

11 Assign an IP address to the TMS interface.

i Click on the Addresses tab.

ii Click on the Create button. The IP Address (Create) form opens.

iii Configure the parameters:

- Address ID
- IP Address
- Prefix Length

iv Click on the OK button. The IP Address (Create) form closes, and a dialog box appears.

v Click on the OK button. The TMS Interface (Create) form reappears with the assigned IP addresses displayed.

12 Click on the OK button. The TMS Interface (Create) form closes, and a dialog box appears.

13 Click on the OK button. The VPRN Service Subscriber (Edit) form reappears with the new TMS interface displayed in the service navigation tree.

14 Click on the OK button. A dialog box appears.

15 Click on the Yes button. The VPRN Service Subscriber (Edit) form closes, and the Manage Services form reappears.

16 Close the Manage Services form.

Procedure 71-65 To implement dual homing using SRRP

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Create the redundant interface used for SRRP out-of-band messaging between the two NEs.



Note 1 — The two sites that participate in the dual homing configuration do not have to be part of the same service.

Note 2 — Ensure that the pair of sites each contains a properly configured subscriber interface and SAPs underneath the group interface that are participating in the redundant configuration.

Note 3 — Ensure that all subscriber interface IP addresses have a gateway address configured on them.

i On the navigation tree, click on the sites to which you need to add the redundant pair; expand the entries for that site.

ii Right-click on Redundant Interfaces for one site of the redundant pair, and choose Create Redundant Interface. The Redundant Interface (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State

iv Click on the Addresses tab.

v Click on the Create button. The IP Address (Create) form opens.

vi Specify IP addresses for the redundant interface on the current and remote sites. Configure the parameters:

- Address ID
- IP Address
- Prefix Length
- Remote IP Address

  This must be on the same subnet as the redundant interface IP address of the current site. For example, if the IP address of the current site is 7.7.7.7, with a prefix length of 24, then the redundant interface IP address of the remote site must be 7.7.7.d, where d is a value from 0 to 255, excluding 7.
- Broadcast Address Format

vii Click on the OK button. The IP Address (Create) form closes, and a dialog box appears.

viii Click on the OK button. The Redundant Interface (Create) form reappears with the assigned redundant interface IP addresses listed.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Redundant Interface (Create) form for the current site closes.

5 Create an SDP spoke binding between the current and remote sites. The Source Interface is the Redundant Interface you created in step 4 and the Tunnel Termination SIte is the remote site. The Return Tunnel must come from the remote site. See Procedure 71-56 for more information.

6 Assign the Redundant Interface to the Group Interface for the current site.

i On the navigation tree under the Subscriber Interface, right-click on the Group Interface you need to use and choose Properties. The VPRN Group Interface (Edit) form opens with the General tab displayed.

ii Click on the Select button in the Redundant Interface panel. The Select Redundant Interface - VPRN Group Interface form opens.

iii Configure the list filter parameters if required and click on the Search button. A list of Redundant Interfaces on the site appears at the bottom of the form.

iv Select the Redundant Interface you created in step 4. The Select Redundant Interface - VPRN Group Interface form closes and the interface you selected appears in the Redundant Interface field.

v Click on the OK button. The VPRN Group Interface (Edit) form closes.

7 Create an SRRP Instance for the current site.

i On the navigation tree under Group Interfaces, right-click on the SRRP Instances item for the current site, and choose Create SRRP Instance. The SRRP Instance (Create) form opens with the General tab displayed.

ii Configure the parameters:

- SRRP ID
- Description
- Administrative State



Note — The SRRP ID value must be the same for the current and remote sites.

iii Click on the Behavior tab.

iv Configure the General parameters:

- Gateway MAC Address Default is 00-00-00-00-00-00.
- Keep Alive Interval
- Priority
- FIB Population Mode

v Configure the Message Path by clicking the Select button adjacent to the Port field. The Select Message Path Pointer - SRRP Instance form opens, displaying the SAPs available on the site. Select the SAP you need to use for the in-band messaging between the sites.

vi Configure the Policy Pointers for the SRRP Instance, if required.

vii Click on the OK button. The SRRP Instance (Create) form closes, and a dialog box appears.

viii Click on the OK button. The VPRN Service (Edit) form reappears with the SRRP Instance displayed.

8 Click on the Turn Up button to activate the SRRP instance.

9 Repeat steps 4 to 8 for the remote site.



Note 1 — When you repeat steps 4 to 8 for the remote site, that site becomes the current site and the previously configured site is the remote site.

Note 2 — After the two sites have been properly set up, you can examine the SRRP peer associations at any time by right-clicking an SRRP Instance in the service's navigation tree. This opens the SRRP Instance - Edit form, which contains a read-only field called SRRP Peer. The Site ID, Service ID, and Operational State of the associated peer appear in this field.

You can also examine the state of an SRRP Instance by checking the Operational Flags field. The flags indicate specific problems that might occur with the SRRP Instance, as follows:

- Duplicate Subscriber IF Address: one of the local subscriber IP addresses is the same as a subscriber IP address on the remote node.
- Redundant Interface Mismatch: the local SRRP instance and remote SRRP instance have mismatched redundant interfaces.
- SAP Mismatch: the local SRRP instance is backing a different set of SAPs than the peer.
- Subnet Mismatch: one of the subnets that SRRP is backing up does not have a match with the peer.
- Dual Master: both SRRP instances are master at the same time.
- SAP Tag Mismatch: the local SRRP instance is backing a set of SAPs with different remote and local tags.
- SRRP ID Mismatch: the peer has a different SRRP instance ID backing the same subnet.

10 Click on the OK button. A dialog box appears.

11 Click on the OK button. The VPRN Service (Edit) form closes.

Procedure 71-66 To create an OSPF sham link

Perform this procedure to create an intra-area OSPF sham link between two VPRN sites. See "OSPF sham link support" in section 71.1 for more information.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service.

4 Click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

5 On the navigation tree, choose the first site that to participate in the sham link. If you need to create the site, perform Procedure 71-3.

6 Choose an L3 access interface for the site. If you need to create the L3 access interface, perform steps 5 to 18 of Procedure 71-22.

7 Configure OSPFv2 for the site. Perform steps 6 to 10 of Procedure 71-50. Ensure that you select substep a in step 8.

8 Right-click on the OSPFv2 icon under the Protocols icon and choose Create Sham Link. The ShamLink (Create) form opens with the General tab displayed.

9 Click on the Select button to configure the Remote Neighbor IP Address parameter. This is the IP Address of the other site participating in the sham link.

10 Click on the Select button in the Interface panel to configure the Interface Name parameter. The Select Interface - ShamLink form opens.

11 Click on the Search button.

12 Choose an interface from the displayed list and click on the OK button. The Select Interface - ShamLink form closes and the ShamLink (Create) form refreshes with the selected Interface Name displayed.

13 Click on the Select button in the Area panel to configure the Area ID parameter. The Select Area - ShamLink form opens.

14 Click on the Search button.

15 Choose an area from the displayed list and click on the OK button. The Select Area - ShamLink form closes and the ShamLink (Create) form refreshes with the selected Area ID displayed.

16 Configure the Administrative State parameter.

17 Click on the Protocol Properties tab.

18 Configure the parameters:

- Metric
- Hello Interval (seconds)
- Router Dead Interval (seconds)
- Retransmission Interval (seconds)
- Transit Delay (seconds)

19 The Authentication tab is configurable, depending on the OSPF version. Click on the Authentication tab to configure authentication for the sham link, if required. Otherwise, go to step 22.

20 Configure the Authentication Type parameter. Perform one of the following:

a Click on the Authentication Type menu button and choose MD5-based Authentication from the drop-down menu.

i Click on the Create button to create an MD5 authentication key. The Md5Key (Create) form opens.

ii Configure the parameters:

- Key Index
- Key
- Re-enter Key

iii Click on the OK button. A dialog box appears.

iv Click on the Yes button. The Md5Key (Create) form closes, and the new authentication key appears in the list.

b Click on the Authentication Type menu button and choose Simple Password from the drop-down menu.

i Click on the Change Password button to enter a password. The Password (Create) form opens.

ii Configure the parameters:

- Password
- Re-enter Password

iii Click on the OK button. A dialog box appears.

iv Click on the Yes button. The Password (Create) form closes.

21 You can click on the Virtual Neighbor tab to view OSPF configuration information on neighbor sites, if required.

22 Click on the OK button. A dialog box appears.

23 Click on the Yes button. The ShamLink (Create) form closes, and the 5620 SAM displays an icon for the new sham link in the navigation tree.

24 Repeat steps 5 to 23 for the second site participating in the sham link.

25 Click on the OK button. A dialog box appears.

26 Click on the Yes button to confirm the action. The VPRN Service (Edit) form closes and the Manage Services form reappears.

27 Click on the Close button to close the Manage Services form.

Procedure 71-67 To run an OAM validation test for a VPRN service

An OAM validator test suite must be created for the tested entity. See chapter 77 for more information about how to create an OAM validator test suite.



Note — As an alternative, you can also run an OAM validation test on the service by performing a One Time Validation. This is a mostly automated procedure and is described in Procedure 77-9.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a service and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

4 Click on the Validate button. If the Validate button is not visible, click on the More Actions button and choose Validate. If an OAM validator test suite is not associated to the service, a dialog box appears. Perform the following steps:

- **i** Click on the OK button to associate the service with an existing OAM validator test suite. The Choose Validator Test Suite form opens.
- **ii** Configure the filter criteria. A list of OAM validator test suites appears.
- **iii** Choose an OAM validator test suite and click on the OK button. The Choose Validator Test Suite form closes.

5 View the State Cause indicators. When the validation test fails, a check mark appears beside the OAM Validation Failure indicator.

6 Click on the Tests tab.

7 Click on the Tested Entity Result tab.

8 Choose an entry and click on the Properties button. The Tested Entity Result (Edit) form opens with the General tab displayed.

9 Click on the Results tab to display the validation test results.

10 If you need to compare two test results from the same type of test, choose the two test results and click on the Compare button; the Difference form opens. Otherwise, go to step 13.

11 Compare the test results.

12 Close the Difference form.

13 Close the Tested Entity Result form.

14 Close the VPRN Service (Edit) form.

15 Close the Manage Services form.

Procedure 71-68 To view the service topology map associated with a VPRN service

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Topology View button. A Topology View dialog box appears.

4 Click on the Yes button to proceed. The Service Topology - map opens.

See chapter 6 for more information about service topology views.

Procedure 71-69 To view the VPRN service operational status

The Aggregated Operational State and State Cause indicators on the General tab of the service management form display information about service faults.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a service and click on the Properties button. The VPRN Service (Edit) form opens.

4 View the Aggregated Operational State and State Cause indicators. When the Aggregated Operational State is Down or Partially Down, a check mark beside the appropriate State Cause indicator identifies the type of associated service fault.

5 Click on the appropriate tab to view or edit an object that is identified as faulty by a State Cause indicator.

6 Click on the Faults tab to view the alarms for the object. The Object Alarms tab is displayed.

7 Click on the Aggregated Alarms tab to view the aggregated alarms for the object. The Aggregated Alarms tab is displayed.

8 Close the VPRN Service (Edit) form.

9 Click on the Close button to close the Manage Services form.

Procedure 71-70 To view DHCPv6 leases

This procedure describes how to view the DHCPv6 prefixes that the server has given out.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 On the navigation tree, click on the site where you need to view DHCPv6 leases; expand the entries for that site.

5 Choose Routing Instance from the navigation tree. The Site (Edit) form opens with the General tab displayed.

6 Click on the RADIUS/DHCP/Diameter tab. The Local DHCP Servers tab is displayed.

7 Click on the DHCP V6 tab. The list of associated DHCPv6 servers is displayed.

8 Choose a DHCPv6 server and click on the Properties button. The Local DHCPv6 Server (Edit) form opens with the General tab displayed.

9 Click on the Show Leases button. If the Show Leases button is not visible, click on the More Actions button and choose Show Leases. The DHCPv6 Server Show Leases form opens.

10 Perform one of the following:

a To view the entire list of leases that are active on the DHCPv6 server, click OK.

b To view the lease information for a specific prefix, enter the IP address in the Prefix parameter for the particular DHCPv6 server and click OK.



Note — If the prefix does not exist in the list of leases, a message displays.

c To view the detailed lease information for a specific prefix, enter the IP address in the Prefix parameter for the particular DHCPv6 server, select the Detail check box, and click OK. The form displays the CLI details for the specific prefix.

11 Close the DHCPv6 Server Show Leases form.

12 Close the Local DHCPv6 Server (Edit) form.

13 Close the Site (Edit) form.

14 Close the VPRN Service (Edit) form.

15 Close the Manage Services form.

Procedure 71-71 To view DHCPv6 log events

This procedure describes how to view lease not owner and pool unknown log events for local DHCPv6 servers.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 On the navigation tree, click on the site where you need to view DHCPv6 log events; expand the entries for that site.

5 Choose Routing Instance from the navigation tree. The Site (Edit) form opens with the General tab displayed.

6 Click on the RADIUS/DHCP/Diameter tab. The Local DHCP Servers tab is displayed.

7 Click on the DHCP V6 tab. The list of associated DHCPv6 servers is displayed.

8 Choose a DHCPv6 server and click on the Properties button. The Local DHCPv6 Server (Edit) form opens with the General tab displayed.

9 Click on the Logs tab. The Lease Not Owner Log and Pool Unknown Log tabs display.

10 Click on the tab for the type of log that you wish to display. Configure the filter criteria and click on the Search button. A list of NE SHCV event logs appears.

11 Configure the filter criteria and click on the Search button. A list of event logs appears.

12 Choose a log entry and click on the Properties button. The Log form opens.

13 View the log entry.

14 Close the Log form.

15 Close the Local DHCPv6 Server (Edit) form.

Procedure 71-72 To modify a VPRN service



Caution 1 — Modifying parameters can be service-affecting.

Caution 2 — The behavior of the VPRN service may become unpredictable if modifications to the configuration affect the IPsec portion of the service configuration. For example, if a VPRN service is configured with IPsec tunnels, IPsec SAPS, and policies are deleted, the service is not deleted from the 5620 SAM and the service will be in an inconsistent state. The IPSEC portion of the VPRN configuration must be deleted using CLI scripts or the CLI before the VPRN service can be deleted from the 5620 SAM.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the general properties of the service displayed on the General tab.

The following tabs list the service elements that can be individually or collectively selected and configured:

- Tests tab — allows the creation and execution of service-specific diagnostic tests
- Sites tab — lists the sites that are included in the service
- L3 Access Interfaces tab — lists the L3 access interfaces that are included in the service
- Spoke SDP Bindings tab — displays the spoke SDP bindings that are associated with the service
- Addresses tab — lists the IP addresses that are associated with the service



Note — You cannot remove an IP address from an interface when the IP address of a static host is defined in the subnet of the interface IP address and the ARP Populate parameter is enabled on the Anti-Spoofing tab.

- Template tab — displays the template used to create the service, if applicable.
- Faults tab — displays the faults associated with the service



Note — Users with the administrator scope of command role can click on the Select button on the Template tab to associate a service template with the service object, if required.

4 Modify the parameters for the service, as required.

To configure items in the tabs that contain lists of service elements, select the items and click on the Properties button.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button to confirm the action. The VPRN Service (Edit) form closes and the Manage Services form reappears.

7 Click on the Close button to close the Manage Services form.

Procedure 71-73 To modify a VPRN service using the topology view

The topology view for a service provides a graphical representation of the various components and their interconnections. You can also use this view to add, modify, or just navigate to service components. This provides an alternative approach to performing these functions from the navigation tree view.

Working from the topology view can expedite the creation of the components, since many of the fields you would ordinarily have to set in the configuration forms will be automatically populated using this approach. The configuration forms can also be accessed directly at any time from this view by right-clicking a component. This allows quick access to conduct more detailed component configuration.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPRN service and click on the Topology View button. The Service Topology map opens.

The remainder of this procedure contains a number of sub-procedures describing the various components that can be viewed, created, or modified from the topology view. These include:

- Creating a new site. Go to step 4.
- Creating site components. Go to step 9.
- Creating spoke SDP bindings. Go to step 36.
- Viewing the route target topology. Go to step 44.

Adding a new site

4 Right-click on any blank space in the service topology map. A contextual menu is displayed. Choose the Create VPRN Site option.

The Select Network Elements form opens.

5 Select one or more sites to add to the service and click OK. The VPRN Site (Create) form for the new site is displayed. If you selected more than one site, the VPRN Site (Multiple Instances) (Create) form for the new sites is displayed.

6 Click on OK. The VPRN Site (Create) (or VPRN Site (Multiple Instances) (Create)) form closes and the new site (or sites) is displayed on the map.

7 If you need to perform detailed configuration of site properties for the new site, right-click the site icon and select Properties from the contextual menu. The VPRN Site (Edit) form opens. See Procedure 71-1 for detailed site configuration information.

8 Return to step 3 for a list of other functions you can perform from the topology view or go to step 46 to finish.

Creating site components

9 Right-click on any site icon in the service topology map. A contextual menu is displayed. You can choose to create one of the following:

- VPRN L3 Access Interface. Go to step 10.
- Tunnel Interface. Go to step 15.
- VPRN Subscriber Interface. Go to step 20.
- Redundant Interface. Go to step 24.
- IP Mirror Interface. Go to step 28.
- Video Interface. Go to step 32.

10 If you choose to create a VPRN L3 Access Interface, then the VPRN L3 Access Interface (Create) form is displayed.

11 Configure the Name parameter on the General tab.

12 Click on the Port tab and assign a port to the interface.

See Procedure 71-22 for detailed information on further configuring the interface, if required.

13 Click OK. The VPRN L3 Access Interface (Create) form closes and the new L3 access interface is displayed in the topology view.

14 Go to step 35.

15 If you choose to create a tunnel interface, then the Tunnel Interface (Create) form is displayed.

16 Configure the Name parameter on the General tab.

17 Click on the Port tab and assign a port to the interface.

See Procedure 29-6 in Chapter 29 for detailed information on further configuring the interface, if required.

18 Click OK. The Tunnel Interface (Create) form closes and the new tunnel interface is displayed in the topology view.

19 Go to step 35.

20 If you choose to create a VPRN Subscriber Interface, then the VPRN Subscriber Interface (Create) form is displayed.

21 Configure the Name parameter for the interface.

See Procedure 71-59 for detailed information on further configuring the interface, if required.

22 Click OK. The VPRN Subscriber Interface (Create) form closes and the new subscriber interface is displayed in the topology view.

23 Go to step 35.

24 If you choose to create a Redundant Interface, then the Redundant Interface (Create) form is displayed.

25 Configure the Name parameter for the interface.

See Procedure 71-65 for detailed information on further configuring the interface, if required.

26 Click OK. The Redundant Interface (Create) form closes and the new redundant interface is displayed in the topology view.

27 Go to step 35.

28 If you choose to create an IP Mirror Interface, then the IP Mirror Interface (Create) form is displayed.

29 Configure the Name parameter for the interface.

See Procedure 71-63 for detailed information on further configuring the interface, if required.

30 Click OK. The IP Mirror Interface (Create) form closes.

31 Go to step 35.

32 If you choose to create a Video Interface, then the Video Interface (Create) form is displayed.

33 Configure the Name parameter for the interface.

See Procedure 30-1 in Chapter 30 for detailed information on further configuring the interface, if required.

34 Click OK. The Video Interface (Create) form closes and the new video interface is displayed in the topology view.

35 Return to step 3 for a list of other functions you can perform from the topology view or go to step 46 to finish.

Creating spoke SDP bindings

36 Select the sites you need to connect in the service topology map and right-click on any one of them. A contextual menu is displayed.



Note — When you create a spoke binding between two sites, the order in which you select them is important. The first site you select will become the source site and the second site will become the destination site. Therefore, it is not recommended that you do a marquee-select in the topology view, since you will not be sure of this hierarchy. Instead, select the sites individually, and hold down the Shift or Ctrl key after your first selection.

37 Select Connect from the contextual menu and choose the Create Spoke SDP Binding option.

The Spoke SDP Binding (Create) form is displayed.



Note — For this function, it is assumed that you clicked on the source site first and then held down the Shift or Ctrl key while right-clicking on the destination site to display the contextual menu.

38 Enable the Auto-Select Transport Tunnel parameter.

39 You can manually configure other parameters here if required, or click on the OK button. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Spoke SDP Binding (Create) form closes and the new binding between the two sites is displayed in the topology view. See Procedure 71-56 for more detailed information on creating and configuring spoke SDP bindings, if required.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. See Chapter 27 for information about how to create the required tunnel. After the tunnel is created, you can repeat this sub-procedure.

40 Assuming that the spoke SDP binding was successfully created in step 39, select the same two sites again in the topology view, although this time do so in the opposite order that you originally selected them. This allows you to create a spoke binding for the return tunnel.

41 Right-click on the second site you selected and choose the Create Spoke SDP Binding ... option from the contextual menu. The Spoke SDP Binding (Create) form is displayed.

42 You can manually configure other parameters here if required, or click on the OK button. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Spoke SDP Binding (Create) form closes and the new return binding between the two sites is displayed in the topology view.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. See Chapter 27 for information about how to create the required tunnel. After the tunnel is created, you can repeat this sub-procedure.

43 Return to step 3 for a list of other functions you can perform from the topology view or go to step 46 to finish.

Viewing the route target topology

44 Right-click on any blank space in the service topology map. A contextual menu is displayed. Choose the Highlight Route Target Topology option.

This option essentially draws dotted lines to represent the route target topology between NEs. For example, for two NEs A and B, if the import and export route targets match, then two dotted lines will be drawn on the map. One will represent the route target going from A to B, and the other from B to A.

45 Return to step 3 for a list of other functions you can perform from the topology view or go to step 46 to finish.

46 Close the Service Topology form.

47 Close the Manage Services form.

Procedure 71-74 To delete a VPRN service



Warning — Deleting a service may result in a service disruption for customers. Consider the implication of deleting the service before proceeding.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 As required, configure the filter criteria to locate the service or range of services to be deleted. A list of services appears.

3 Choose a service or a range of services from the list.



Note 1 — You cannot delete a VPRN service when IPsec security policies, interfaces, or tunnels are configured. See the appropriate node documentation for more information about modifying or deleting IPsec configurations.

For example, if a VPRN service is configured with IPsec tunnels, IPsec SAPS, and policies is deleted, the service is not deleted from the 5620 SAM and the service will be in an inconsistent state. The IPSEC portion of the VPRN configuration must be deleted using the CLI scripts or through the CLI before the VPRN service can be deleted from the 5620 SAM.

Note 2 — The L3 interface properties for the IPSEC SAP cannot be configured using the 5620 SAM.

4 Click on the Delete button. A warning form opens. This form is dynamic based on the priority of the service. Perform one of the following:

a For services with a low priority, go to Step 5.

b For services with a medium priority, configure the “Enter the highest priority of the service being deleted” text field by typing: Medium. Go to Step 5.

c For services with a high priority, configure the “Enter the highest priority of the service being deleted” text field by typing: High. Go to step 5.

5 For all services regardless of how their priority is configured, acknowledge the check box that prompts you confirm that you understand the implications of deleting the service.



Note — If you select multiple services with different priorities, you must enter the highest priority level of selected services before you can delete the services.

6 Click on the Yes button to confirm the action. The service is deleted and removed from the list.

7 Click on the Close button to close the Manage Services form.

72 — PW routing and dynamic MS-PW service management

72.1 PW routing and dynamic MS-PW service management overview *72-2*

72.2 Workflow to configure PW routing and dynamic MS-PW services *72-3*

72.3 PW routing and dynamic MS-PW service management procedures *72-5*

72.1 PW routing and dynamic MS-PW service management overview

Service providers require a solution for interconnecting customer sites that span different domains, such as MAN-WAN or Inter-AS (in the same Service Provider or Inter-Provider). The 5620 SAM supports two methods for interconnecting customers sites:

- PW routing
- MS-PW routing

PW routing

The 5620 SAM supports inter-domain services for VLL through the use of VLL spoke switching, which allows creation of a VLL service by cross-connecting two spoke SDPs. However, this requires statically configuring the PW switching points at the gateway S-PEs between domains. See "VLL spoke switching" in chapter 67 for more information.

Static PW routing is supported on the 7450 ESS, 7710 SR, and 7750 SR, and on a Release 11.0 or later 7950 XRS.

MS-PW routing

Multi-Segment Pseudo-Wire routing provides solutions for inter-domain services by using dynamic MS-PW routing and signaling, in which the switching points are automatically instantiated in the Switching-Provider Edge (S-PE) NEs. The path of the MS-PW is dynamically signaled end-to-end by T-LDP, using PW routing information stored in the S-PEs by MP-BGP. Per-PW configuration is only required at the endpoints of the MS-PW in the Termination-Provider Edge (T-PE) NEs.

Dynamic MS-PWs are characterized by the following:

- They are supported for VLL Epipe services
- Dynamic and static routes, as well as explicit paths for MS-PWs are supported
- Dynamic MS-PWs may be established across LDP or RFC 3107 labeled BGP SDPs
- Dynamic MS-PWs may be used as a part of a set of PWs for PW redundancy, including MC-LAG. Diverse routes for the active and standby MS-PWs can be configured by using explicit paths, or dynamically by using a BGP route distinguisher.
- Diverse routes for the active and standby MS-PWs can be achieved by using explicit paths or dynamically using a BGP route distinguisher.

Dynamic MS-PWs are supported on Release 9.0 R3 and later 7450 ESS, 7710 SR, 7750 SR chassis types that support Epipe service creation, and on the 7950 XRS.

Dynamic MP-PW services

Spoke SDP FEC configuration will bind a service to an existing Service Distribution Point (SDP), using a dynamic MS-PW. When using dynamic MS-PWs, the particular SDP to bind to is automatically selected based on the Target Attachment Individual Identifier (TAII) and the path to use, specified under the Spoke SDP FEC. The selected SDP will terminate on the first hop S-PE of the MS-PW. Therefore, an SDP should be defined that can reach the first hop of the MS-PW. The NE creates a spoke SDP binding to associate an SDP with a service. If the required SDP does not exist, the NE creates one based on the parameters specified in the spoke SDP FEC, for example, the SAII/TAII, Path, or PW template. The Creation Mode attribute for such an SDP indicates Multi-Segment PW.

This differs from the regular spoke SDP binding creation in that it creates a spoke SDP binding using a PW with the FEC128. However, the Spoke SDP FEC enables PWs with other FEC types to be used.

Spoke SDP FEC configuration is currently only applicable to an Epipe site. It can be configured under the Epipe service or at a service endpoint of an Epipe site, with or without ICB. The creation under an Epipe service is demonstrated in Procedure 72-3.

72.2 Workflow to configure PW routing and dynamic MS-PW services

The following workflow lists the high-level steps required to configure PW routing and dynamic MS-PW services. Enabling MS-PW support requires configuration in the following areas:

- network commissioning
- SR NE pre-provisioning
- dynamic MS-PW service
- optional PW routing and MS-Service tasks

Network commissioning

1 To use PW routing to establish dynamic pseudo-wires from source to destination, without using static routes and a specified path:

   a Enable BGP on the routing instance of the required node. See Procedure 23-1 for more information.

   b Configure the BGP Family parameter to include the options MS-PW and IPv4. This must be done on the BGP site, associated BGP groups, and BGP peers.

   Refer to the following procedures:

   - BGP Site configuration: See step 25 in Procedure 23-2
   - BGP Peer Group configuration: See step 22 in Procedure 23-4
   - BGP Peers configuration: See step 21 in Procedure 23-5

2 If more than one equal cost route is required for the PW routing, configure the following:

a In the routing instance for the required NE, set the Maximum Number of Equal Cost Routes parameter to a value greater than 1. See step 19 in Procedure 22-1.

b For the required BGP Site, set the Multi Path parameter to a value greater than 1. See step 9 in Procedure 23-2.

3 Configure a routing policy with the Family parameter having the MS-PW option enabled. This will then be exported under the BGP site. See step 26 in Procedure 22-15.

4 If path diversity is required for primary/standby MS-PWs, perform the following:

a Configure a routing policy having multiple statement entries, each associated with a different community, from a different neighbour, with family including MS-PW and a local preference. The communities configured here are used further on in the procedure when configuring a MS-PW local prefix. See Procedure 22-15 for more information, with attention to steps 28 and 29.

b Import the above policy under the BGP site. See Procedure 23-2 for more information.

5 If there are ASBRs, set Next Hop Self to True under each peer group. For example, set one for the inner-AS and one for the external-AS. Without this setting, the SDPs created by MS-PW routing only reach to the BGP interface's IP address, but not the system ID. See step 11 in Procedure 23-4. Refer also to Chapter 71 for information on ASBRs.

6 If all T-PEs and S-PEs are within the same AS, then the S-PEs must be configured as route reflectors (RR). Perform the following:

a Set the Cluster ID parameter on the BGP site or BGP peer group that includes the T-PEs as BGP peers on the S-PE. See step 4 in Procedure 23-2.



Note — Two T-PEs can not be configured as BGP peers to each other. They must be configured as BGP peers of the RR.

b Configure a routing policy with Advertise Next Hop Self set to true and Action set to Accept, and then export this policy under the BGP site. See step 9 in Procedure 22-15.

This completes the summary of essential network commissioning requirements.

SR NE pre-provisioning

7 Configure PW routing:

a using the navigation tree (see Procedure 72-1)

b using the Manage Services form (see Procedure 72-2)

Configure a dynamic MS-PW service

8 Configure a dynamic MS-PW service using PW routing. See Procedure 72-3.

Optional PW routing and MS-Service tasks

9 As required, perform one or more of the following:

a On-demand resync of the MS-PW routing table for a specified NE is supported and can be accessed from a number of places in the 5620 SAM. See Procedure 72-4 for information on displaying MS-PW routing tables.

b Conduct various spoke SDP FEC operations from the endpoint of an Epipe site. See Procedure 72-5.

c Discover and manage MS-PW switching sites. See Procedure 72-6.

d Run an OAM VCCV Ping or Trace validation test for the MS-PW service. See Procedure 72-7.

72.3 PW routing and dynamic MS-PW service management procedures

This section contains the configuration and management procedures required to configure PW routing and dynamic MS-PW services using the 5620 SAM.

Procedure 72-1 To configure PW routing using the navigation tree

This procedure creates service routes for the MS-PW routing on the NE using the navigation tree. Configuration of the following steps is required on the T-PE or S-PE, as detailed.

1 Right-click on a discovered device in the navigation tree and choose Properties from the contextual menu. The properties form for the device opens.

2 Click on the Globals tab and then the Service sub-tab.

3 Click on the PW Routing sub-tab and then its General sub-tab.

4 Configure the parameters:

- SPE Address
- Boot Timer (seconds)
- Retry Timer (seconds)
- Retry Count

The SPE Address must be unique in the network. This parameter must be configured on all T-PEs and S-PEs that are involved in this PW routing.

The Number of BGP Routes, Number of Static Routes, Number of Local Routes, and Number of Host Routes attributes are for information only and can be resync-ed from the NE.

5 Click on the Local Prefixes sub-tab under PW Routing.

6 Click the Create button. The PW Routing NE Local Prefix (Create) form opens.

7 Configure the Local Prefix parameter.

You must configure this parameter to enable the MS-PW routing configuration on a T-PE node. This Local Prefix is also used in other portions of the MS-PW configuration, such as setting static routes on the remote T-PE or intermediate S-PEs, and setting Source Attachment Individual Identifier (SAII) and Target Attachment Individual Identifier (TAII) addresses on a spoke SDP FEC on the T-PE.

8 Click the Create button in the BGP RD panel. The PW Routing NE BGP RD (Create) form opens.

A route distinguisher must be configured to enable this local prefix to be advertised by MP-BGP to the network.

9 Configure the Route Distinguisher parameter.

10 Click the Select button to configure the BGP Community parameter.

The Community can only be selected from the list. Members were created as part of the routing policy configuration in Procedure 22-15 and importing the routing policy under the BGP site in Procedure 23-2.

11 Click on OK.

12 Repeat steps 8 to 11 to create up to four route distinguishers per local prefix.

13 Repeat steps 5 to 13 to create up to 16 local prefixes per NE. The local prefixes you create must be unique in the network.

14 Click the OK button. The PW Routing NE Local Prefix (Create) form closes.

At this point the NE can start to advertise the defined local prefix to its BGP peers.

15 Click on the Static Routes sub-tab under PW Routing.

16 Click the Create button. The PW Routing NE Static Route Configuration (Create) form opens.

A static route can be configured on both the T-PE and S-PE, based on your requirements.

17 Click the Select button to configure the Target T-PE's PW Address parameter.

This specifies the local prefix defined in the remote T-PE. It can be selected from a managed T-PE or S-PE, or directly entered.

18 Click the Select button to configure the Next Hop parameter.

This specifies the system IP address of the next-hop S-PE or T-PE. It can be selected from a managed T-PE or directly entered.

19 Click the OK button. The PW Routing NE Static Route Configuration (Create) form closes.

At this point the NE can start to advertise the defined static route to its BGP peers.

20 Click on the Configured Paths sub-tab under PW Routing if you need to configure an explicit path. All such configured paths are displayed in the list.

The path should be configured on the T-PEs, which is then used in the spoke SDP FEC to establish a pseudo-wire through the specified path.

21 Click the Create button. The PW Routing NE Path Configuration (Create) form opens, with the General tab displayed.

22 Specify a Path Name.

23 Click the Create button in the Hops panel. The PW Routing Hop (Create) form opens.

24 Configure the Hop ID parameter.

25 Configure the Hop Address parameter.

This specifies the system IP address of the next-hop S-PE or T-PE (where the T-LDP session to a given S-PE terminates). It can be entered directly or chosen from the managed S-PE or T-PE by clicking the Select button.

26 Click the OK button. The PW Routing Hop (Create) form closes.

27 Repeat steps 23 to 26 to create the required hops.

28 Click the OK button. The PW Routing NE Path Configuration (Create) form closes.

Procedure 72-2 To create, modify, or view a PW routing NE configuration using the Manage Services form

Perform this procedure to create, modify, or view a PW Routing NE configuration using the Manage PW Routing NE Configuration form. This is an alternative approach to the SR NE pre-provisioning section detailed in the procedural workflow in Procedure 72-1.

1 Choose Manage→Service→PW Routing NE Configuration from the 5620 SAM main menu. The Manage PW Routing NE Configuration form opens.

2 Configure the drop-down filter criteria for PW Routing NE Path Configuration and click the Search button. A list of PW Routing NE configurations appears in the form.

3 Choose the required PW Routing NE configuration and click on the Properties button. The PW Routing NE Configuration (Edit) form opens with the General tab displayed.

4 Configure the parameters, as required:

- SPE Address
- Boot Timer (seconds)
- Retry Timer (seconds)
- Retry Count

5 Click the Local Prefixes tab.

6 Click the Search button and then Properties for an existing prefix, or the Create button for a new one from this tab. If you are creating a new local prefix, configure the Local Prefix parameter on the General tab of the PW Routing NE Local Prefix form.

Whether you are working with an existing or a new local prefix, you can also search for or create new BGP RDs for the current prefix.

7 Click the Search button and then Properties for an existing BGP RD, or the Create button for a new one from this tab. If you are creating a new BGP RD, configure the Route Distinguisher and Community parameters in the PW Routing NE BGP RD (Create) form.

8 Click OK to close the PW Routing NE BGP RD (Create) form. The new BGP RD appears in the list.

9 If there are local spoke SDP FECs associated with this local prefix, click the Local Spoke SDP FECs tab to list them. Select an item from the list and click Properties to view the object information, if required.

10 Click the Static Routes tab.

11 Click the Search button and then Properties for an existing static route, or the Create button for a new one from this tab. If you are creating a static route, configure the Target T-PE's PW Address and Next Hop parameters in the PW Routing NE Static Route Configuration (Create) form.

12 Click OK to close the PW Routing NE Static Route Configuration (Create) form. The new static route appears in the list.

13 Click the Configured Paths tab.

14 Click the Search button and then Properties for an existing path configuration, or the Create button for a new one from this tab. If you are creating a new path configuration, configure the Path Name parameter on the General tab of the PW Routing NE Path Configuration form.

Whether you are working with an existing or a new path configuration, you can also search for or create new Hops for the current configuration.

15 Click the Search button and then Properties for an existing Hop, or the Create button for a new one from this tab. If you are creating a new Hop, configure the Hop ID and Hop Address parameters in the PW Routing Hop (Create) form.

16 Click OK to close the PW Routing Hop (Create) form. The new Hop appears in the list.

17 If there are spoke SDP FECs associated with this path configuration, click the Spoke SDP FECs tab to list them. Select an item from the list and click Properties to view the object information, if required.

18 Click OK to close PW Routing NE Configuration (Edit) form.

Procedure 72-3 To configure a dynamic MS-PW service using PW routing

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria for Service→VLL (VLL)→Epipe Service→(Epipe). A list of services appears at the bottom of the Manage Services form.

3 Choose the required VLL Epipe service that contains the T-PE site and click on the Properties button. The Epipe Service (Edit) form opens with the General tab displayed.

4 Click on the Spoke SDP FECs tab.

5 Click the Create button. The Spoke SDP FEC (Create) form opens.



Note — Only one spoke can be configured on the terminating site, including both regular spoke SDP bindings and spoke SDP FECs.

6 Configure the parameters:

- PW ID
- Auto-Assign ID
- SAII Address
- SAII AC ID
- Auto Config
- TAII Address
- TAII AC ID
- Administrative State
- Signaling Type
- Retry Timer (seconds)
- Retry Count
- Path
- PW Template

The Auto Config parameter enables automatic endpoint configuration. This allows the configuration of a spoke SDP endpoint without specifying the TAII associated with that spoke SDP. In this mode, the far end T-PE actively initiates MS-PW signaling and will send the initial label mapping message using T-LDP, while the T-PE for which Auto Config is specified will act as the passive T-PE. The Auto Config parameter cannot be enabled if the Signaling Type is set to Master or if the TAII Address is specified.

If you are going to use SAII and TAII addresses instead of Auto Config, then you must decide which method will be used for the PW routing.

- For dynamic PW routing, the local prefix associated with the SAII/TAIl address should be configured with a route distinguisher, with an optional community (refer to steps 8 to 12 in Procedure 72-1). The SAII and TAII addresses must be unique in the network.
- For static routing, the local prefix should be associated with static routes configured under PW routing (refer to steps 15 to 19 in Procedure 72-1). A spoke SDP FEC cannot be turned up if no local prefix is configured under PW routing.
- When using a specified path, the Path parameter must be configured. The associated Select button allows you to select a path that will be used for this spoke SDP and which is configured under PW Routing. If no path is configured, then each next hop of the MS-PW used by the spoke SDP will be chosen locally at each S-PE and T-PE, using dynamic PW routing.

7 If redundancy is required, specify an Endpoint using the associated Select button.

8 Configure the parameters:

- Inter-Chassis Backup
- Precedence
- Active State
- Enable PW Standby Signaling Slave

9 Click the Return Spoke SDP FEC tab to configure a return spoke SDP FEC, as required.

This tab is only displayed when the TAII Address configured in step 6 was set by selection for the current spoke SDP FEC.

10 Configure the PW ID parameter for the return spoke SDP FEC and click Apply.

When a valid PW ID for the return spoke SDP FEC is entered, additional parameters are displayed. If the PW ID is not valid, then the return spoke SDP FEC will not be created.

11 Configure the parameters:

- Signaling Type
- Auto Config
- Path
- PW Template
- Set ICB

12 Specify an Endpoint using the associated Select button.

When the return spoke SDP FEC is created, it will have corresponding attributes such as the SAII and TAII Address values and AC ID cross-matching with the current spoke SDP FEC.

13 Click OK to apply the configurations and close the Spoke SDP FEC (Create) form.

When a spoke SDP FEC is successfully created, it will be listed under the Spoke SDP FECs tab for this Epipe site.

14 Select the spoke SDP FEC from the list and click Properties.

The spoke SDP FEC should contain the following tabs: General, Spoke SDP Associated, Tests, and Faults.

The Spoke SDP Associated tab will list the spoke SDP bindings created by using this Spoke SDP FEC for MS-PW routing. All such spoke SDP bindings have their Creation Mode attribute set as Multi-Segment PW. The related SDP FEC Auto-bind tab shows the associated SAII or TAII defined in the Spoke SDP FEC.

The Faults tab will display any mis-configuration alarms associated with this spoke SDP FEC.

15 Close the Epipe Service (Edit) form.

When the configuration for both T-PEs is complete, the NEs can start negotiating and establishing the spoke SDP bindings from T-PE to S-PE and from S-PE to T-PE.

Procedure 72-4 To display MS-PW routing tables

On-demand resync of the MS-PW routing table for a specified NE is supported and can be accessed from a number of places in the 5620 SAM.

1 Select an applicable NE from one of the following locations:

- Navigation tree
- Physical Topology map
- Service Tunnel map

2 Right-click the NE to open the pop-up menu.

3 Click on the Show MS-PW Routes and select one of the following show commands:

- BGP
- Service

The Service Routing rtr BGP or Service Routing rtr Service form opens accordingly. The requested routing table information is presented, along with a detailed status/error report.

4 Close the Service Routing rtr report form.

Procedure 72-5 To perform spoke SDP FEC operations from an endpoint

Perform this procedure to conduct various spoke SDP FEC operations from the endpoint of an Epipe site.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria for Service→VLL (VLL)→Epipe Service→(Epipe). A list of services appears at the bottom of the Manage Services form.

3 Choose the required VLL Epipe service that contains the primary and backup spoke SDP FECs and click on the Properties button. The Epipe Service (Edit) form opens with the General tab displayed.

4 Expand the Spoke SDP FECs item under the required Epipe site in the navigation tree.

5 Right-click the required Spoke SDP FEC. A pop-up menu appears. Select the required action:

- Force Switchover
- Clear Forced Switchover
- Turn Up
- Shut Down
- Delete
- Resync
- Properties

The Forced Switchover and Clear Forced Switchover options are only applicable where the Epipe site has been configured for redundancy, as detailed in Procedure 72-3. The switchover applies to the primary and backup spoke SDP FECs configured on the Epipe site.

6 Close the Epipe Service (Edit) form.

Procedure 72-6 To discover and manage MS-PW switching sites

With PW routing configured on T-PEs and S-PEs, and spoke SDP FECs configured on the T-PEs, the SR 7x50 will establish the pseudo-wires between T-PEs. This includes creating switching sites between two T-PEs. A switching site for MS-PW is a read-only site (nothing can be modified) and it cannot be deleted. It is controlled by the NE.

Use the following method to discover such sites, if required.



Note 1 — The switching sites and spoke SDP bindings created by MS-PW routing are tagged with their Creation Mode attribute indicating Multi-Segment PW (as opposed to Manual for non-MS-PW entities).

Note 2 — When a switching site is discovered, the associated spoke SDP bindings under it are also discovered and re-synced. The 5620 SAM will create a composite service and connector(s) if there are matching spoke SDP bindings found in other Epipe services (based on cross-matching of the spoke SDP ingress/egress labels). The related service is added to the newly-created composite service.

1 Conduct an RCA Audit to discover switching sites, if required. This is done within the Epipe service that contains the T-PEs having MS-PW configured. The audit will find all MS-PW switching sites associated with T-PEs in this service and provide management solutions.

Refer to Procedure 80-1 for details on configuring an RCA audit.

2 Perform Procedure 80-2.

Procedure 72-7 To conduct MS-PW routing OAM tests

The MS-PW routing configuration can be tested using OAM VCCV Ping and Trace tests.

1 To conduct a VCCV Ping test refer to Procedure 32-23.

The test can be created either from the Service Test Manager or from a configured Epipe service, Epipe site, or a Spoke SDP FEC.

If you choose a spoke SDP binding created by MS-PW routing, the VCCV ping is specifically for MS-PW, and the SAII and TAII parameters will be auto-filled. This allows you to conduct a MS-PW VCCV Ping on an S-PE.

If the test is created from a configured Spoke SDP FEC, the test object will be auto-filled with the configured spoke SDP FEC.

Alternatively, if the test is created from the Service Test Manager, an Epipe service, or an Epipe site (both the termination site and the switching site), then you must select a spoke SDP FEC (only for T-PE) or a spoke SDP binding of type FEC 129 created by the MS-PW routing.

2 To conduct a VCCV Trace test refer to Procedure 32-24.

The test can be created either from the Service Test Manager or from a configured Epipe service, Epipe site, or a Spoke SDP FEC.

If the test is created from a configured Spoke SDP FEC, the test object will be auto-filled with the configured spoke SDP FEC.

Alternatively, if the test is created from the Service Test Manager, an Epipe service, or an Epipe site (both the termination site and the switching site), then you must select a spoke SDP FEC (only for T-PE) or a spoke SDP binding of type FEC 129 created by the MS-PW routing.



Note 1 — When configuring either a VCCV Ping or VCCV Trace test for dynamic MS-PW from an S-PE, the Reply Type must be set to IP.

Note 2 — If the selected spoke SDP binding is created by MS-PW routing, you can only conduct a VCCV ping for MS-PW FEC129, not for FEC128.

Note 3 — If a PW template is used in the Spoke SDP FEC configuration, it must have its Enable Control Word parameter enabled, since both VCCV Ping and Trace require Control Word support.

3 To create a Test Suite refer to Procedures 77-4 and 77-8.

A Test suite can be generated based on the selected policy for a specified VLL Epipe service.

If the selected policy has its Entity Type set to VLL Service, then the VCCV Ping and VCCV Trace tests that are generated will adhere to the following:

- No tests are generated for spoke SDP bindings created by MS-PW routing.
- Both VCCV Ping and VCCV Trace tests for MS-PW will be generated if there are spoke SDP FECs in the specified Epipe service.

If the selected policy has its Entity Type set to Service Connector, then there is also no test generated for the spoke SDP bindings created by MS-PW.

73 — Service PW template policy management

73.1 Service PW template policies overview *73-2*

73.2 Workflow to configure PW template policies *73-2*

73.3 Service PW template policies procedures *73-2*

73.1 Service PW template policies overview

Service PW templates policies enable you to automatically create SDP bindings on NEs that support BGP AD VPLS. PW templates contain the configuration to use when the 5620 SAM creates SDP bindings automatically through BGP AD. PW templates use the 5620 SAM policy distribution model to distribute the template to the NEs.

To prevent unwanted service disruptions, NEs do not automatically reconfigure SDP bindings when a change is made to the PW template from which they were generated. You can manually trigger a template re-evaluation to cause the NEs to re-configure SDPs to match the configuration in the template. PW templates can be re-evaluated at three levels:

- service
- service site
- local definition of PW template policy

When you re-evaluate a PW template from the local definition of the PW template policy, the 5620 SAM re-evaluates the selected template for all of the VPLSs on the selected site.

When you re-evaluate a PW template from the service site, the 5620 SAM re-evaluates the selected template on the selected service site.

When you re-evaluate a PW template from the service, the 5620 SAM re-evaluates the selected template on all sites in the VPLS.

73.2 Workflow to configure PW template policies

The following workflow lists the high-level steps required to create and manage a service PW template policy.

1 Create a PW template policy. See Procedure 73-1.

2 Release and distribute the PW template policy to each NE that is or will be a component of the VPLS or BGP VPLS. See Procedure 73-2.

3 Reevaluate PW template when a configuration change is made to the PW template. See Procedure 73-3.

73.3 Service PW template policies procedures

The following procedure describes how to manage service PW template policies.

Procedure 73-1 To create a PW template policy

1 Choose Manage→Service→Service PW Template Policies from the 5620 SAM main menu. The Manage Service PW Template Policies form opens.

2 Click on the Create button. The Service PW Template (Create) form opens with the General tab displayed.

3 Perform one of the following:

a Click on the Populate from Pseudowire button. If this button is not visible, click on the More Actions button and choose Populate from Pseudowire.

This allows you to populate the Service PW Template form using an existing pseudowire (SDP Binding) as a base.

i After choosing Populate from Pseudowire, the Select a Pseudowire form opens.

ii Click on the Search button.

iii Choose the required pseudowire from the displayed list.

iv Click on OK. All of the relevant values are copied into the Service PW Template form.

v Go to step 22.

b Populate the form manually.

i Configure the parameters:

- Policy ID
- Auto-Assign ID
- Description
- Enable Hash Label
- Enable Signal Capability
- Use Provisioned SDP
- Force VLAN VC Forwarding
- Enable Control Word
- VC Type
- Collect Stats
- Block On Peer Fault



Note 1 — The Block On Peer Fault parameter takes effect only when PW status signaling is enabled.

Note 2 — The Block On Peer Fault parameter is not configurable on a spoke SDP that is on an MC LAG or an endpoint.

ii Select an Accounting Policy, if required, by clicking on the Select button. The Select Accounting Policy form opens.

iii Select an accounting policy and click OK, or create a new one by clicking on the Create button.

4 Click on the MAC tab.

5 Configure the following parameters, as required:

- MAC Learning
- MAC Aging
- Discard Unknown Source
- Limit MAC Move
- MAC Pinning
- VLAN VC Tag
- MAC Address Limit
- Restrict Protected Source (MAC)
- Restrict Protected Source Action (MAC)
- Auto Learn MAC Protect (MAC)

6 Click on the Split Horizon Group tab.

7 Configure the following parameters, as required:

- Split Horizon Group Name
- Description
- Restrict Protected Source (Split Horizon Group)
- Restrict Protected Source Action (Split Horizon Group)
- Restrict Unprotected Destination
- Auto Learn MAC Protect (Split Horizon Group)

8 Click on the Ingress Filters tab.

9 Configure the Ingress Filter Type parameter, if required.

10 Click on the Egress Filters tab.

11 Configure the Egress Filter Type parameter, if required.

12 Click on the IGMP tab.

13 Configure the following parameters, as required:

- IGMP Version
- IGMP Fast Leave
- IGMP Import Policy
- IGMP Last Member Interval (deciseconds)
- IGMP Max Number Groups
- IGMP Max Number Sources Per Group
- IGMP General Query Interval (seconds)
- IGMP Query Response Interval (seconds)
- IGMP Robust Count
- IGMP Send Queries

14 Click on the QoS tab.

15 Configure the required parameters in the Ingress Forwarding Plane Redirect panel:

i Click on the Network Policy Select button to assign a policy to the PW template. The Select Network Policy form opens.

ii Choose a policy from the list and click on the OK button. The Network Policy form closes.

iii Click on the Ingress Queue Group Template Policy Select button to assign a policy to the PW template. The Select Ingress Queue Group Template Policy form opens.

iv Choose a policy from the list and click on the OK button. The Ingress Queue Group Template Policy form closes.

v Configure the Instance ID parameter.

16 Click on the Tunnel Admin Groups tab.



Note — You can apply the inclusion or exclusion of tunnel administrative groups only if you set the Use Provisioned SDP parameter to true in step 3b i.

17 Click on the tunnel administrative groups that you need to include in the PW template policy in the Included Admin Groups-Unassigned panel. You can choose multiple groups by holding down the CTRL key when you click on the group.

18 Click on the right arrow to move the selected administrative groups into the Included Admin Groups-Assigned panel. You can move an assigned administrative group to the unassigned portion of the form if required, by selecting the group and clicking on the left arrow.

19 Click on the tunnel administrative groups that you need to exclude from the PW template policy in the Excluded Admin Groups-Unassigned panel. You can choose multiple groups by holding down the CTRL key when you click on the group.

20 Click the right arrow to move the selected administrative groups into the Excluded Admin Groups-Assigned panel. You can move an assigned tunnel administrative group to the unassigned portion of the form, if required, by selecting the group and clicking the left arrow

21 Configure the required parameters in the Egress Port Redirect panel:

- **i** Click on the Network Policy Select button to assign a policy to the PW template. The Select Network Policy form opens.
- **ii** Choose a policy from the list and click on the OK button. The Network Policy form closes.
- **iii** Click on the Egress Queue Group Template Policy Select button to assign a policy to the PW template. The Select Egress Queue Group Template Policy form opens.
- **iv** Choose a policy from the list and click on the OK button. The Egress Queue Group Template Policy form closes.
- **v** Configure the Instance ID parameter.

22 Click on the OK button to confirm your changes. The Service PW Template - Local Policy - (Edit) form closes.

23 Click on the OK button to close the Service PW Template - Global Policy form.

Procedure 73-2 To distribute a PW template policy

Use this procedure to manually distribute PW template policies that are used by BGP AD capable NEs and to configure the distribution mode of local policies.

When you distribute a global policy, local policies using the Sync With Global distribution mode allow the NE to receive the policy.



Note — Local policies using the Local Edit Only distribution mode do not allow the NE to receive the distribution of a global policy. You must ensure that the policy distribution mode for the local policy is set to Sync With Global if you need the NE to receive the distribution of a global policy.

1 Choose Manage→Service→Service PW Template Policies from the 5620 SAM main menu. The Manage Service PW Template Policies form opens.

2 Click on the Search button.

3 Choose the policy or policies that you need to distribute.

4 Perform steps 5 to 24 in Procedure 42-1 to release and distribute the Service PW Template Policy.

Procedure 73-3 To reevaluate a PW template policy on a local definition after a configuration change

Perform the following procedure to cause the NEs to re-configure SDPs to match the configuration in the template when a PW template policy is modified. This causes a re-evaluation of the selected template for all VPLS services on the selected NE.

You can also reevaluate a PW template policy at the service and service site levels.

1 Choose Manage→Service→Service PW Template Policies from the 5620 SAM main menu. The Manage Service PW Template Policies form opens.

2 Choose a PW template policy and click on the Properties button. The Service PW Template Policy (Edit) form opens with the General tab displayed.

3 Click on the Local Definitions tab.

4 Choose the NE on which you need to re-evaluate the PW template policy. The Service PW Template - Local Policy (Edit) form opens with the General tab displayed.

5 Click on the Re-evaluate PW Template button to run an evaluation of the modified template. If this button is not visible, click the More Actions button and choose Re-evaluate PW Template. The 5620 SAM performs a re-evaluation of the selected template for all VPLS services on the selected NE.

6 A dialog box appears indicating if the re-evaluation was successful. If it was not, the reason for the failure is displayed. If you make any subsequent modifications, you can re-evaluate the template again. Click on the OK button.

7 Close the Service PW Template - Local Policy - (Edit) form.

8 Click on the OK button to close the Service PW Template - Global Policy form.

74 — Composite service management

74.1 Composite service management overview *74-2*

74.2 Sample composite service configuration *74-7*

74.3 Workflow to create a composite service *74-8*

74.4 Composite service management procedures *74-9*

74.1 Composite service management overview

A composite service is a set of linked services. Composite service functionality supports complex applications that require a combination of services, such as VLAN connections to an HVPLS, an IES spoke into a VPLS, or a VPRN-to-VPLS interconnection.

Services that are owned by different customers can be connected to form a composite service. An example is an HVPLS in which the core VPLS belongs to one customer and the satellite VPLS instances belong to other customers. An HVPLS is considered to be a composite service by the 5620 SAM.

Composite services consist of customer services, called SCs in the context of a composite service, and connectors. A connector is a bidirectional logical link between two SCs, such as a pair of PW spokes that carry traffic in opposite directions between VLL and VPLS instances, a dot1q-encapsulated link between a VLAN and a VPLS, or an internal cross-connect.

The term SCP describes a type of connector endpoint. In the case of the services that are available on the 7210 SAS, 7450 ESS, 7710 SR, 7750 SR, or the 7950 XRS, an SCP is a service interface or SAP. For L2 switches, an SCP may be a network interface, such as an uplink port.

Composite services exist only in the context of the 5620 SAM and are configured through the 5620 SAM GUI or an OSS application. They are unknown to individual network devices. To simplify composite service configuration and to ensure that non-5620 SAM device configuration does not disrupt the management of composite services, the following rules apply to the creation, deletion, modification, and presentation of composite services.

- A composite service can have zero SCs.
- A composite service can have zero connectors.
- Two connected SCs can belong to only one composite service.
- A connector between two SCs belongs to only one composite service.
- An SC cannot be removed from a composite service until its connector to the composite service is removed.
- A group of connected services can be moved from one composite service to another.

The 5620 SAM supports composite-service configuration using the following methods.

- Tabbed configuration forms with an embedded navigation tree that provides a logical, hierarchical view of the composite service and acts as a configuration interface. When you right-click on an object in the navigation tree, a menu specific to the object appears. When you choose an object in the menu, the related configuration form opens.
- Connector creation and configuration from within the composite service's flat topology view
- Pre-configured template. A user who is assigned the service management scope of command role can create a composite-service template. The service management user can also create a connector template. See "Managing

templates" in the *5620 SAM Scripts and Templates Developer Guide* for more information about the administrative tasks associated with creating and using templates.

If a service that is specified for inclusion in a composite service does not currently belong to a composite service, it is added to the composite service regardless of its administrative or operational state. If the specified service is part of an existing composite service, it can be moved to a different composite service. However, SCs that are connected to the specified service are also moved to the new composite service upon confirmation of the action by the 5620 SAM operator. The 5620 SAM performs no such action confirmation for OSS applications.

Services within a composite service can have the same service ID, service type, and customer ID. For example, a VPLS with service ID 5 on one NE and an IES service with service ID 5 on another NE can be combined to create a composite service.

Hierarchical organization of composite services

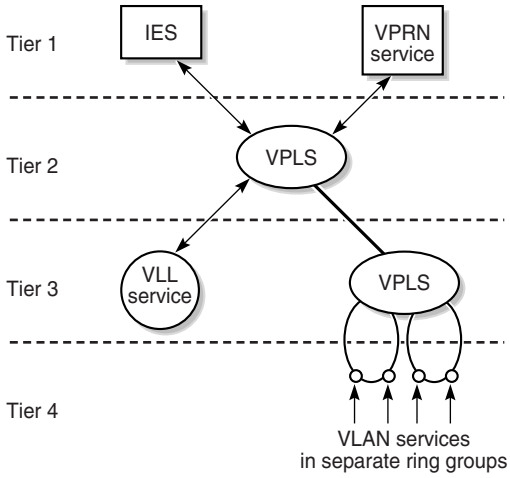
The 5620 SAM organizes the SCs in a composite service by tiers within a hierarchy during network discovery and for display purposes. When you add an SC to a composite service, the 5620 SAM assigns a default tier value to the SC according to the service type. Table 74-1 lists the default tiers for different service types.

Table 74-1 Default tiers for service types

Service type	Default tier
IES and VPRN	1
VPLS and MVPLS	2
VLL	3
VLAN	4

The default tier values reflect common deployment configurations. Figure 74-1 shows a composite service hierarchy. SCs are not restricted to the default tiers, as in the case of the VPLS in Tier 3 that forms an HVPLS with the VPLS in Tier 2.

Figure 74-1 Default SC tier assignments



You can change the tier of an SC at any time and can specify a value other than one of the defaults that the 5620 SAM assigns; composite services can have many tiers.

The tier value of an SC determines the relative position of the SC within a composite service topology map. The 5620 SAM displays SCs in rows by tier, in numerical order from the top of the panel downward, beginning with tier 1.

You can move SC icons in a composite service topology map from one tier to another for a customized view, then use the Rearrange by Service Tiers button to organize the SC icons in the map panel according to tier.

Caution — The composite service topology map is redrawn when you click on the Rearrange by Service Tiers button, and you cannot revert to the former layout of the composite service topology map.

See chapter 6 for more information about 5620 SAM map management.

Network discovery of composite services

The 5620 SAM associates SCs and connectors with composite services during network discovery. The following rules apply to this process.

- When the 5620 SAM discovers a valid connector between two services that do not belong to a composite service, a composite service that contains the services and connector is automatically created.
- When the 5620 SAM discovers a valid connector between two services and one of the services belongs to a composite service, the other service is added as an SC of the composite service.
- When the 5620 SAM discovers a valid connector between two services and the two services are SCs of different composite services, an alarm is raised and the connector is excluded from the 5620 SAM database.

The 5620 SAM assigns a default tier value to a service upon creation and to a new SC during network discovery. The tiered hierarchy provides a common framework for service configurations that are provisioned through the 5620 SAM and CLI. A 5620 SAM operator can assign a different tier value to an SC after discovery.

A composite service has Aggregated Operational State and Service Component Degraded status indicators. The General tab of the Composite Service management form displays these indicators.

The Aggregated Operational State indicator has four possible values: Up, Down, Partially Down, and Unknown. The value is derived from the aggregated SC operational states as follows.

- Up—All SCs are operationally up
- Partially Down—At least one SC is operationally down
- Down—All SCs are operationally down
- Unknown—The status of at least one SC is undetermined

The Service Component Degraded indicator shows whether there is an operational flag set on any of the service sites under this composite service.

Connector types

The following types of connectors join SCs in a composite service:

- SCP-to-SCP
- internal cross-connect
- PW spoke
- routed VPLS



Note — The 5620 SAM does not create connectors between mesh SDP bindings.

SCP-to-SCP connectors

SCP-to-SCP connectors can join any two SC types that have service interfaces on the same device or on different devices. A connector between VPLS and VPRN SAPs is an SCP-to-SCP connector, as is a connector between a dot1q-encapsulated VPLS SAP and L2 switch uplink port in a VLAN ring group. Table 74-2 describes the supported encapsulation types.

Table 74-2 Supported encapsulation types

SAP type	Encapsulation type
Ethernet	dot1q
	QinQ
	Null

(1 of 2)

SAP type	Encapsulation type
ATM	VPI/VCI
	VPI
FR	DLCI
SONET/SDH	BCP Null
	BCP dot1q
	IPCP
	PPP Auto
	cHDLC
	WAN Mirror
LAG	Null
	dot1q

(2 of 2)

The operational status of an SCP-to-SCP connector depends on the operational status of its endpoints. An alarm raised against one of the endpoints causes an alarm to be raised against the connector. Such alarms are aggregated within the composite service.

Internal cross-connect connectors

An internal cross-connect connector can join any SC types. It uses a CCAG to join two SCs that have SAPs or network interfaces on the same device. This functionality is available in the 7450 ESS, 7710 SR, and 7750 SR. The following rules apply to internal cross-connect connectors.

- A SAP can be connected to another SAP or to a network interface using a CCAG.
- When a SAP or network interface is deleted, the connector associated with it is also deleted.
- The deletion of an internal cross-connect connector causes the associated interfaces and SAPs to be deleted.

The operational state of an internal cross-connect connector depends on the operational state of the CCAG. An alarm raised against the CCAG causes an alarm to be raised against the connector. Such alarms are aggregated within the composite service.

PW spoke connectors

A PW spoke connector generally joins VPLS instances to create an HVPLS. In the 7210 SAS-M, 7210 SAS-X, 7450 ESS, 7710 SR, 7750 SR, and 7950 XRS, a PW spoke can, for example, connect IES and VPLS instances to provide distributed Internet access service. The endpoints of a PW spoke connector must be on different devices. PW spoke connectors are subject to restrictions on the SC types that they can join. Table 74-3 shows the SC types that can be linked by PW spoke connectors.

Table 74-3 Valid PW spoke interconnections

SC type	Valid PW spoke SC interconnections
VLL	IES, VPLS
VLAN	—
VPLS	IES, VLL, VPLS
MVPLS	MVPLS
IES	VLL, VPLS
VPRN	VLL, VPLS

The operational state of a PW spoke connector depends on the operational state of the underlying SDP bindings. An alarm raised against one of the SDP bindings causes an alarm to be raised against the connector. Such alarms are aggregated within the composite service.

Routed VPLS connectors

A routed VPLS connector joins an L3 access interface within an IES or VPRN service context to a VPLS or I-VPLS on the same site. When an IES or VPRN IP interface is bound to a VPLS site name, the site name cannot be bound to another IP interface. Although an IES or VPRN IP interface can only be bound to a single VPLS site, the service context that contains the IP interface can have other IP interfaces bound to other VPLS sites. Both the IES or VPRN IP interface and VPLS site must be located on the same NE.

If a VPLS site name does not exist within the system, the binding between the IP interface and the VPLS site remains operationally down until a VPLS site name is assigned to the VPLS site. When an IP interface is bound to a VPLS site, the operational state of the binding depends on the operational state of the VPLS site, or whether the IP interface binding is enabled on the VPLS site.

The operational state of the routed VPLS connector depends on the operational state of the binding and the operational state of the L3 IP interface.

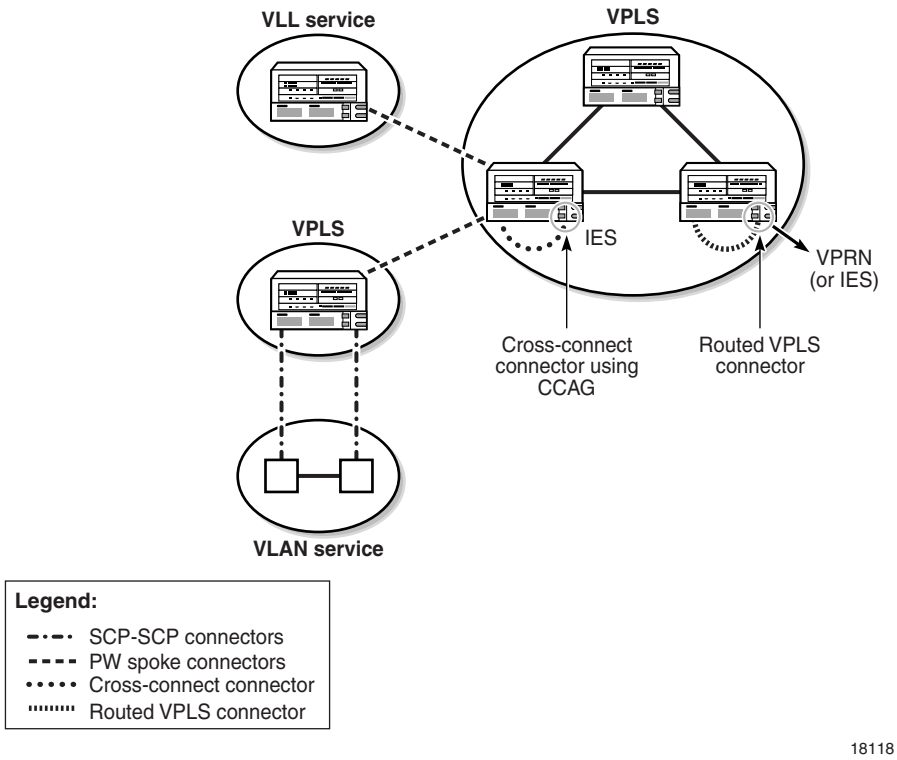
The routed VPLS connector function is supported for IOM3 cards in the following devices:

- Release 8.0 R4 or later 7450 ESS in mixed mode
- Release 8.0 R4 or later 7750 SR
- Release 8.0 R5 or later 7750 SR-c4
- Release 6.0 or later 7705 SAR, all variants
- 7950 XRS

74.2 Sample composite service configuration

Figure 74-2 shows a sample composite service configuration that involves a variety of customer services and uses the three SC connector types.

Figure 74-2 Sample composite service configuration



74.3 Workflow to create a composite service

The following workflow lists the high-level steps required to create a composite service. As a prerequisite for creating a composite service, this workflow assumes the following:

- a group or customer with the required user access privileges has been configured.
- the IP or IP/MPLS core network exists.
- any required service tunnels are created including the static or dynamic LSP required to create the service tunnel; see Procedure 27-1 for more information.
- the access ports for the service are created; see chapter 16 for more information.
- any required pre-defined routing, QoS, scheduling, filter, accounting, and time of day suite policies are created; see chapter 42 for more information. You do not have to create pre-defined policies if policies are created on a per-service basis.

- any required MP-BGP for PE-to-PE routing is configured; see chapter 23 for more information about protocol configuration.
- the other network services that are to be the SCs of the composite service are created.

1 As required, modify the default system preferences for composite services such as specifying if composite services are auto-discovered or if service alarms are aggregated for composite services.

2 Create composite service.

i Define the general properties for the composite service. See Procedure 74-1 for more information.

ii Specify the services for inclusion in the composite service. You can specify multiple services in one operation. See Procedure 74-2 for more information.

iii Create connectors to link the SCs of the composite service. See Procedures 74-3, 74-4, 74-5, and 74-6 for more information.

iv Turn up the composite service.

3 As required, run an OAM validation test for the composite service. See Procedure 74-7 for more information. Alternatively, you can also run a One Time Validation on the composite service. See Procedure 77-9 for more information.

4 As required, force a manual rediscovery of all composite services in the 5620 SAM to discover new service connectors that would add SCs to an existing composite service, or for new service connectors that would connect together two SCs to create a new composite service. See Procedure 74-8 for more information.

5 Manage a composite service.

i View the service topology map associated with a composite service. See Procedure 74-9 for more information.

ii As required, modify a composite service:

- using the navigation tree; see Procedure 74-10 for more information
- using the flat topology view; see Procedure 74-11 for more information

iii As required, delete a composite service. See Procedure 74-12 for more information.

74.4 Composite service management procedures

Use the following procedures to perform composite service creation and management tasks.

Procedure 74-1 To create a composite service

1 Choose Manage→Service→Composite Services from the 5620 SAM main menu. The Manage Composite Services form opens.

2 Click on the Create button. The Composite Service (Create) form opens with the General tab displayed.

3 Configure the parameters.

- Composite ID
- Auto-Assign ID
- Name
- Description

The Composite ID parameter is configurable only if the Auto-Assign ID parameter is disabled.

4 Click on the Apply button. The form refreshes with additional parameters.

5 Configure the parameters:

- Current OLC State
- Revert OLC State

6 Perform one of the following:

a Add an SC to the composite service. Perform steps 4 to 11 of Procedure 74-2.

b Complete composite service creation if SCs are to be added later. Go to step 7.

7 Click on the OK button. The CompositeService - *Service Name* (Edit) form closes and a dialog box appears.

8 Click on the Yes button to confirm the action. The Manage Composite Services form reappears with the new composite service displayed in the list.

9 Close the Manage Composite Services form.

Procedure 74-2 To add services to a composite service

1 Choose Manage→Service→Composite Services from the 5620 SAM main menu. The Manage Composite Services form opens.

2 Configure the filter criteria and click the Search button. A list of composite services appears.

3 Select a composite service and click on the Properties button. The Composite Service (Edit) form opens with the General tab displayed.

4 In the navigation tree, right-click on the Services icon and choose Add Services. The Add Services form opens.



Note — You can also create a service for inclusion in the composite service by right-clicking on the Services icon and choosing Create *Service Type*.

5 Click on the Search button. A list of available services is displayed.

6 Select a service and click on the OK button. You can select multiple services. The service or services are added below the Services object in the navigation tree.

7 Perform one of the following:

- **a** Add a connector to the composite service. Go to step 8.
- **b** Complete composite service creation if connectors are to be created later. Go to step 9.

8 Perform one of the following to add a connector to the composite service:

- **a** Create a cross connect connector. Perform steps 4 to 21 of Procedure 74-3.
- **b** Create a routed VPLS connector. Perform steps 4 to 20 of Procedure 74-6.
- **c** Create an SCP connector. Perform steps 4 to 22 of Procedure 74-4.
- **d** Create SpokeConnector. Perform steps 4 to 29 of Procedure 74-5.

9 Click on the OK button. The CompositeService - *Service Name* (Edit) form closes and a dialog box appears.

10 Click on the Yes button to confirm the action. The Manage Composite Services form reappears with the new composite service displayed in the list.

11 Close the Manage Composite Services form.

Procedure 74-3 To create a cross connect connector

1 Choose Manage→Service→Composite Services from the 5620 SAM main menu. The Manage Composite Services form opens.

2 Configure the filter criteria and click the Search button. A list of composite services appears.

3 Select a composite service and click on the Properties button. The Composite Service (Edit) form opens with the General tab displayed.

4 In the navigation tree, right-click on the Connectors icon and choose Create CrossConnect. The Cross Connect (Create) form opens.



Note — The service endpoints of a cross-connect connector must be on the same NE.

5 Configure the parameters:

- Name
- Description

6 Click on the Select button in the Service A panel to choose an SC to associate with the connector. The Select Service A - Cross Connect form opens with a list of available SCs displayed.

7 Choose an SC and click on the OK button. The Select Service A - Cross Connect form closes and the Cross Connect (Create) form refreshes.

8 Click on the Select button in the Service B panel to choose an SC to associate with the connector. The Select Service B - Cross Connect form opens with a list of available SCs displayed.

9 Choose an SC and click on the OK button. The Select Service B - Cross Connect form closes and the Cross Connect (Create) form refreshes.

10 Click on the Select button in the Site A panel to choose a site to associate with the connector. The Select Site - Cross Connect form opens with a list of available sites displayed.

11 Choose a site and click on the OK button. The Select Site - Cross Connect form closes and the Cross Connect (Create) form refreshes.

12 Click on the Select button in the Site B panel to choose an SC to associate with the connector. The Select Site - Cross Connect form opens with a list of available sites displayed.

13 Choose a site and click on the OK button. The Select Site - Cross Connect form closes and the Cross Connect (Create) form refreshes.

14 Click on the Transport tab.

15 Click on the Select button to choose a CCAG for the connector. The Select CCAG - Cross Connect form opens with a list of available CCAGs displayed.

16 Choose a CCAG and click on the OK button. The Select CCAG - Cross Connect (Create) form closes and the Cross Connect (Create) form refreshes.

17 Configure the parameters.

- CC ID
- Auto-Assign ID

18 Click on the OK button. The Cross Connect (Create) form closes and the CompositeService - *Service Name* (Edit) form refreshes.

19 Click on the OK button. A dialog box appears.

20 Click on the Yes button to confirm the action. The Manage Composite Services form reappears with the new composite service displayed in the list.

21 Close the Manage Composite Services form.

Procedure 74-4 To create an SCP connector

1 Choose Manage→Service→Composite Services from the 5620 SAM main menu. The Manage Composite Services form opens.

2 Configure the filter criteria and click the Search button. A list of composite services appears.

3 Select a composite service and click on the Properties button. The Composite Service (Edit) form opens with the General tab displayed.

4 In the navigation tree, right-click on the Connectors icon and choose Create ScpConnector. The ScpConnector (Create) form opens.

5 Configure the parameters:

- Name
- Description

6 Click on the Select button in the Service A panel to choose an SC to associate with the connector. The Select Service A - ScpConnector form opens with a list of available SCs displayed.

7 Select an SC and click on the OK button. The Select Service A - Scp Connector (Create) form closes and the ScpConnector (Create) form refreshes.

8 Click on the Select button in the Service B panel to choose an SC to associate with the connector. The Select Service B - ScpConnector form opens with a list of available SCs displayed.

9 Select an SC and click on the OK button. The Select Service B - Scp Connector (Create) form closes and the ScpConnector (Create) form refreshes.

10 Click on the Select button in the Site A panel to choose a site to associate with the connector. The Select Site - ScpConnector form opens with a list of available sites displayed.

11 Select a site and click on the OK button. The Select Site - Scp Connector (Create) form closes and the ScpConnector (Create) form refreshes.

12 Click on the Select button in the Site B panel to choose a site to associate with the connector. The Select Site - ScpConnector form opens with a list of available sites displayed.

13 Select a site and click on the OK button. The Select Site - Scp Connector form closes and the ScpConnector (Create) form refreshes.

14 Click on the Service Connection Point tab.

15 Click on the Select button in the Service Connection Point A panel to choose an SCP to associate with the connector. The Select Service Connection Point A - Scp Connector form opens with a list of available SCPs displayed.

16 Select an SCP and click on the OK button. The Select Service Connection Point A - Scp Connector form closes and the ScpConnector (Create) form refreshes.

17 Click on the Select button in the Service Connection Point B panel to choose an SCP to associate with the connector. The Select Service Connection Point B - Scp Connector form opens with a list of available SCPs displayed.

18 Select an SCP and click on the OK button. The Select Service Connection Point B - Scp Connector form closes and the ScpConnector (Create) form refreshes.

19 Click on the OK button. the ScpConnector (Create) form closes and the CompositeService - *Service Name* (Edit) form refreshes.

20 Click on the OK button. A dialog box appears.

21 Click on the Yes button to confirm the action. The Manage Composite Services form reappears with the new composite service displayed in the list.

22 Close the Manage Composite Services form.

Procedure 74-5 To create a spoke connector

1 Choose Manage→Service→Composite Services from the 5620 SAM main menu. The Manage Composite Services form opens.

2 Configure the filter criteria and click the Search button. A list of composite services appears.

3 Select a composite service and click on the Properties button. The Composite Service (Edit) form opens with the General tab displayed.

4 In the navigation tree, right-click on the Connectors icon and choose Create ScpConnector. The SpokeConnector (Create) form opens.



Note — The service endpoints of a spoke connector must be on different NEs.

5 Configure the parameters:

- Name
- Description

6 Click on the Select button in the Service A panel to choose an SC to associate with the connector. The Select Service A - Spoke Connector form opens with a list of available SCs displayed.

7 Select an SC and click on the OK button. The Select Service A - Spoke Connector (Create) form closes and the SpokeConnector (Create) form refreshes.

8 Click on the Select button in the Service B panel to choose an SC to associate with the connector. The Select Service B - Spoke Connector form opens with a list of available SCs displayed.

9 Select an SC and click on the OK button. The Select Service B - Spoke Connector form closes and the SpokeConnector (Create) form refreshes.

10 Click on the Select button in the Site A panel to choose a site from service A to associate with the connector. The Select Site - Spoke Connector form opens with a list of available sites displayed.

11 Select a site and click on the OK button. The Select Site - Spoke Connector form closes and the SpokeConnector (Create) form refreshes.

12 Click on the Select button in the Site B panel to choose a site from service B to associate with the connector. The Select Site - Spoke Connector form opens with a list of available sites displayed.

13 Select a site and click on the OK button. The Select Site - Spoke Connector form closes and the SpokeConnector (Create) form refreshes.

14 Click on the Transport tab.

15 Configure the parameters.

- VC ID
- Auto-Assign ID
- Auto Select Tunnels
- Transport Type

The Transport Type parameter is configurable when the Auto Select Tunnels parameter is enabled.

16 If the Auto Select Tunnels parameter is enabled, go to step 21.

17 Click on the Select button in the Tunnel A panel to choose a service tunnel to associate with the connector. The Select Tunnel From Site A - Spoke Connector form opens with a list of available service tunnels displayed.

18 Select a tunnel and click on the OK button. The Select Tunnel From Site A - Spoke Connector form closes and the SpokeConnector (Create) form refreshes.

19 Click on the Select button in the Tunnel B panel to choose a service tunnel to associate with the connector. The Select Tunnel From Site B - Spoke Connector (Create) form opens with a list of available service tunnels displayed.

20 Select a tunnel and click on the OK button. The Select Tunnel From Site B - Spoke Connector (Create) form closes and the SpokeConnector (Create) form refreshes.

21 The First L3 Access Interface panel is present, if one of the SCs in the composite service is an IES. If the First L3 Access Interface panel is not present, go to step 26.

22 Click on the Select button in the First L3 Access Interface panel to choose an access interface to associate with the spoke connector. The Select First L3 Access Interface - Spoke Connector (Create) form opens with a list of available L3 access interfaces displayed.

23 The Second L3 Access Interface panel is present, if another of the SCs in the composite service is an IES. If the Second L3 Access Interface panel is not present, go to step 26.

24 Click on the Select button in the Second L3 Access Interface panel to choose an access interface to associate with the spoke connector. The Select Second L3 Access Interface - Spoke Connector (Create) form opens with a list of available L3 access interfaces displayed.

25 Select an L3 access interface and click on the OK button. The Select L3 Access Interface - Spoke Connector (Create) form closes and the SpokeConnector (Create) form refreshes.

26 Click on the OK button. The SpokeConnector (Create) form closes and the CompositeService - *Service Name* (Edit) form refreshes.

27 Click on the OK button. A dialog box appears.

28 Click on the Yes button to confirm the action. The Manage Composite Services form reappears with the new composite service displayed in the list.

29 Close the Manage Composite Services form.

Procedure 74-6 To create a routed VPLS connector

1 Choose Manage→Service→Composite Services from the 5620 SAM main menu. The Manage Composite Services form opens.

2 Configure the filter criteria and click the Search button. A list of composite services appears.

3 Select a composite service and click on the Properties button. The Composite Service (Edit) form opens with the General tab displayed.

4 In the navigation tree, right-click on the Connectors icon and choose Create RoutedVplsConnector. The RoutedVplsConnector (Create) form opens.

5 Configure the parameters:

- Name
- Description

6 Click on the Select button in the Service A panel to choose an SC to associate with the connector. The Select Service A - RoutedVplsConnector form opens with a list of available SCs displayed.

7 Select an SC and click on the OK button. The Select Service A - RoutedVplsConnector form closes and the RoutedVplsConnector (Create) form refreshes.

8 Click on the Select button in the Service B panel to choose an SC to associate with the connector. The Select Service B - RoutedVplsConnector form opens with a list of available SCs displayed.

9 Select an SC and click on the OK button. The Select Service B - RoutedVplsConnector form closes and the RoutedVplsConnector (Create) form refreshes.

10 Click on the Select button in the Site A panel to choose a site to associate with the connector. The Select Site - RoutedVplsConnector form opens with a list of available sites displayed.

11 Select a site and click on the OK button. The Select Site - RoutedVplsConnector form closes and the RoutedVplsConnector (Create) form refreshes.

12 Click on the Select button in the Site B panel to choose a site to associate with the connector. The Select Site - RoutedVplsConnector form opens with a list of available sites displayed.

13 Select a site and click on the OK button. The Select Site - RoutedVplsConnector form closes and the RoutedVplsConnector (Create) form refreshes.



Note — The sites that you select in steps 11 and 13 must be located on the same NE.

14 Click on the Routed-VPLS L3 Connection Point tab.

15 Click on the Select button to choose an interface for the connector. The Select L3 Access Interface - RoutedVplsConnector form opens with a list of available L3 Access Interfaces displayed.

16 Select an L3 Access Interface and click on the OK button. The RoutedVplsConnector (Create) form refreshes.

17 Click on the OK button. The RoutedVplsConnector (Create) form closes and the CompositeService - *Service Name* (Edit) form refreshes.

18 Click on the OK button. A dialog box appears.

19 Click on the Yes button to confirm the action. The Manage Composite Services form reappears with the new composite service displayed in the list.

20 Close the Manage Composite Services form.

Procedure 74-7 To run an OAM validation test for a composite service

A validator test suite must be created for the tested entity. See chapter 77 for more information about how to create a validator test suite.



Note — As an alternative, you can also run an OAM validation test on the composite service by performing a One Time Validation. This is a mostly automated procedure and is described in Procedure 77-9.

1 Choose Manage→Service→Composite Services from the 5620 SAM main menu. The Manage Composite Services form opens.

2 Configure the filter criteria and click Search. A list of composite services appears in the Manage Composite Services form.

3 Select a composite service and click on the Properties button. The Composite Service (Edit) form opens with the General tab displayed.

4 Click on the Action button and select Validate. If a validator test suite is not associated to the composite service, a dialog box appears. Perform the following steps:

   i Click on the OK button to associate the composite service with an existing validator test suite. The Choose Validator Test Suite form appears.

   ii Configure the filter criteria. A list of validator test suites appears.

   iii Select a validator test suite and click on the OK button. The Choose Validator Test Suite form closes.

5 View the Operational Flags indicators. If the validation test fails, a check mark appears beside the OAM Validation Failed indicator.

6 Click on the Tests tab.

7 Click on the Tested Entity Result tab.

8 Select an entry and click on the Properties button. The Tested Entity Result form opens and displays information about the validation test.

9 Close the Tested Entity Result form.

10 Close the Composite Service (Edit) form.

11 Close the Manage Composite Services form.

Procedure 74-8 To rediscover composite services

Complete this procedure to force a manual rediscovery of all composite services in the 5620 SAM. The Rediscover Composite Services command performs a network discovery that looks for new service connectors that would add SCs to an existing composite service, or for new service connectors that would connect together two SCs to create a new composite service.



Note — If the Auto Discover Composite Services system preference is enabled, composite services are rediscovered as part of routine network discovery in the 5620 SAM. See Procedure 64-2 for more information.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Composite Services form opens.

2 Click on the Rediscover Composite Services button.

3 A warning form appears. Click on the Yes button to start the rediscovery.

4 A progress bar appears, indicating the status of the rediscovery process. Upon completion, an information form appears, indicating the number of composite services and connectors discovered. Click on Ok to close the form.

5 Click on the Close button to close the Manage Composite Services form.

Procedure 74-9 To view the service topology map associated with a composite service

1 Choose Manage→Service→Composite Services from the 5620 SAM main menu. The Manage Composite Services form opens.

2 Configure the filter criteria. A list of composite services appears at the bottom of the Manage Composite Services form.

3 Select a composite service and perform one of the following steps:

   a Click on the Topology View button. A Composite Service Topology - *Service Name* map opens.

   b Click on the Topology View Flat button. A Composite Service Flat Topology - *Service Name* map opens. The Flat Topology map is a flattened view of a composite service, meaning that all the service objects are displayed simultaneously, along with the service sites, access interfaces, and the links or groups of links between them.

   See chapter 6 for more information about composite service topology views.

Procedure 74-10 To modify a composite service using the navigation tree



Caution — Modifying parameters can be service-affecting.



Note — You can also modify composite service components and add service connectors from the flat topology view. See Procedure 74-11.

1 Choose Manage→Service→Composite Services from the 5620 SAM main menu. The Manage Composite Services form opens.

2 Configure the filter criteria. A list of composite services appears at the bottom of the Manage Composite Services form.

3 Select a composite service and click on the Properties button. The CompositeService - *Service Name* (Edit) form opens with the General tab displayed.

4 To configure parameters for an item, in the navigation tree, select and right-click on the item, and choose Properties from the contextual menu.

Using the contextual menu, you can also:

- Add SCs and connectors to a composite service
- Create services for inclusion in the composite service. When you create services by using the contextual menu, the services are automatically added to the composite service.
- Remove SCs and connectors from a composite service
- Move SCs to another composite service
- Delete SCs



Warning — Deleting an SC is not the same as removing an SC from a composite service. Deleting an SC removes the service from the 5620 SAM database. To avoid a service outage, be certain of the action that you are taking.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button to confirm the action. The CompositeService - *Service Name* (Edit) form closes and the Manage Composite Services form reappears.

7 Click on the Close button to close the Manage Composite Services form.

Procedure 74-11 To modify a composite service using the flat topology view

You can modify composite service components and add service connectors from the flat topology view. The main advantage of creating connectors using the flat topology view is that most of the parameters in the associated configuration forms are automatically populated when you select an item in the map.



Caution — Modifying parameters can be service-affecting.



Note — You can also modify and add composite service components using the navigation tree. Refer to Procedure 74-10.

1 Choose Manage→Service→Composite Services from the 5620 SAM main menu. The Manage Composite Services form opens.

2 Configure the filter criteria. A list of composite services appears at the bottom of the Manage Composite Services form.

3 Select a composite service and click on the Properties button. The CompositeService - *Service Name* (Edit) form opens with the General tab displayed.

4 Click the Flat Topology View button. The Composite Service Flat Topology map opens.

5 To configure parameters for any item on the map, right-click on the item, and choose Properties from the contextual menu. The configuration form for the item is displayed.

6 Edit the parameters as required. Refer to Procedure 74-1 for detailed configuration information on creating and configuring components.

7 Add service connectors to the composite service, if required.

Depending on the sites or ports you select, when you right-click on a component, the contextual menu contains one or more of the following choices:

- Create Cross Connect. Go to step 8.
- Create Routed Vpls Connector. Go to step 9.
- Create Scp Connector. Go to step 10.
- Create Spoke Connector. Go to step 11.

Click on the required item in the contextual menu and proceed to the associated step indicated in this list.



Note — If you need to modify any of the automatically-populated parameters in the associated configuration forms while creating these connectors, refer to Procedure 74-10 for detailed information.

8 To create a Cross Connect Connector:

i Select the two site icons that you want to create the Cross Connect Connector for. These icons represent the same physical NE that exists in two separate services, since service endpoints of a Cross Connect Connector must be on the same NE.

ii Right-click on either of the icons and select Create Cross Connect from the contextual menu.

The CrossConnect (Create) form opens with the General tab displayed.

iii Configure the parameters.

- Name
- Description (optional)

iv Click on the Transport tab.

v Click on the Select button to choose a CCAG for the connector. The Select CCAG - Cross Connect form opens with a list of available CCAGs displayed.

vi Select a CCAG and click on the OK button. The Select CCAG - Cross Connect (Create) form closes and the CrossConnect (Create) form refreshes.

vii Click on the OK button. The CrossConnect (Create) form closes and the new Cross Connect Connector is displayed on the map.

viii Go to step 15.

9 To create a Routed Vpls Connector:

i Select a VPLS site icon and an L3 Access Interface icon that you want to create the Routed Vpls Connector for. These icons must belong to the same NE.

ii Right-click on either of the icons and select Create Routed Vpls Connector from the contextual menu.

The RoutedVplsConnector (Create) form opens with the General tab displayed.

iii Configure the parameters.

- Name
- Description (optional)

iv Click on the OK button. The RoutedVplsConnector (Create) form closes and the new Routed Vpls Connector is displayed on the map.

v Go to step 15.

10 To create a Scp Connector:

i Select the port icons for the two sites that you want to create the Scp Connector for.

ii Right-click on either of the icons and select Create Scp Connector from the contextual menu.

The ScpConnector (Create) form opens with the General tab displayed.

iii Configure the parameters.

- Name
- Description (optional)

iv Click on the OK button. The ScpConnector (Create) form closes and the new Scp Connector is displayed on the map.

v Go to step 15.

11 To create a Spoke Connector:

i Select the two site icons that you want to create the Spoke Connector for. These icons must be two different NEs that exist in two separate services.

ii Right-click on either of the icons and select Create Spoke Connector from the contextual menu.

The SpokeConnector (Create) form opens with the General tab displayed.

iii Configure the parameters.

- Name
- Description (optional)

iv Click on the OK button. The SpokeConnector (Create) form closes and the new Spoke Connector is displayed on the map.

12 Create new services within the composite service view, if required.

i Right-click on the flat topology map background and choose Create from the menu. A list of services appears.

ii Click on the service type you want to create. The appropriate Service (Create) form appears.

iii Configure the parameters for the service as required and then click on the OK button in the Service (Create) form.

See the appropriate service management chapter for information about creating a specific service type.

iv The Service (Create) form closes and the new service is displayed on the map.

13 Add services to the composite service, if required.

i Right-click on the flat topology map background and choose Add→Service(s) from the menu. An Add Services - Composite Services form appears.

ii Configure the filter criteria and click on the Search button. A list of services appears at the bottom of the Add Services - Composite Services form.

iii Select a service and click on the OK button. The Add Services - Composite Services form closes and the service is displayed on the map. If the service includes service sites, the sites are also displayed on the map.

14 Add service sites to an existing service in the composite service, if required.

i Right-click on the flat topology map background and choose Add→Service Site(s) from the menu. A Find Service form appears.

ii Configure the filter criteria and click on the Search button. A list of services that are already part of the composite service appears at the bottom of the Find Service form.

iii Select a service and click on the OK button. The Find Service form closes and a Select Network Elements form appears with a list of available NEs.

iv Select one or more NEs and then click on the OK button. A Service Site (Create) form appears. If more than one NE is selected, a Service Site, Multiple Instances (Create) form appears.

v Configure the service site and click on the OK button. The new service site is displayed on the map.

See the appropriate service management chapter for information about configuring a specific service site type.

15 Click on the OK button in the CompositeService - *Service Name* (Edit) form. A dialog box appears.

16 Click on the Yes button to confirm your changes. The CompositeService - *Service Name* (Edit) form closes and the Manage Composite Services form reappears.

17 Click on the Close button to close the Manage Composite Services form.

Procedure 74-12 To delete a composite service



Warning — Deleting a service may result in a service disruption for customers. Consider the implication of deleting the service before proceeding.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 As required, configure the filter criteria to locate the service or range of services to be deleted. A list of services appears at the bottom of the Manage Services form.

3 Choose a service or a range of services from the list.

4 Click on the Delete button. A warning form appears. This form is dynamic based on the priority of the service. Perform one of the following:

   a For services with a low priority, go to Step 5.

   b For services with a medium priority, configure the "Enter the highest priority of the service being deleted" text field by typing: Medium. Go to Step 5.

   c For services with a high priority, configure the "Enter the highest priority of the service being deleted" text field by typing: High. Go to step 5.

5 For all services regardless of how their priority is configured, acknowledge the check box that prompts you confirm that you understand the implications of deleting the service.



Note — If you select multiple services with different priorities, you must enter the highest priority level of selected services before you can delete the services.

6 Click on the Yes button to confirm the action. The service is deleted and removed from the list.

7 Click on the Close button to close the Manage Services form.

75 — Dynamic service management

75.1 Dynamic service management overview *75-2*

75.2 Dynamically-created objects *75-3*

75.3 Workflow to create dynamic services *75-4*

75.4 Dynamic service management procedures *75-4*

75.1 Dynamic service management overview

A dynamic service is a service in which sites are created using information contained in RADIUS Change of Authorization messages instead of manual operator input.

The 7450 ESS in mixed mode, Release 11.0 or later, and the 7750 SR, Release 11.0 or later, support dynamic service creation for the following service types:

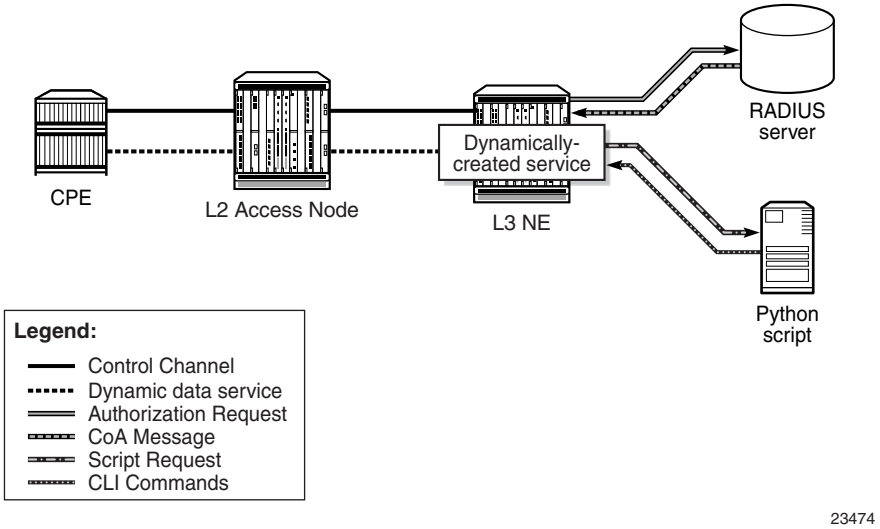
- Epipe
- IES
- VPLS
- VPRN

Dynamic service structure

The creation of a dynamic service is triggered by a CPE device establishing a control channel (PPPoE, IPoE, or DHCP) with an L3 NE. The control channel is authenticated using RADIUS, and the RADIUS server sends Access-Accept or Change of Authorization messages that contain the parameters for the dynamic service required by the triggering device.

The L3 NE passes the information from the RADIUS messages to a Python script, which returns CLI commands that create the required dynamic sites on the NE. Figure 75-1 shows a basic dynamic service.

Figure 75-1 Basic dynamic service



When the control channel fails - for example, when the CPE device is removed - the NE deletes any dynamic services that were created for the control channel.

75.2 Dynamically-created objects

Network objects in a dynamic service are read-only on the NE and in the 5620 SAM, and cannot be modified except through RADIUS CoA messages. As a result, some operations are not supported on dynamically-created sites. This section describes the unsupported operations.

Dynamically created service sites are discovered and synchronized with the 5620 SAM in the same manner as manually created service sites. A service that contains a dynamically created object has the Contains Dynamically Created Sites parameter enabled, and cannot be deleted until the dynamically created object is removed from the service.

Unsupported operations

Table 75-1 describes the operations that cannot be performed on dynamically created objects.

Table 75-1 Unsupported operations on dynamically created objects

Operation	Description
Object configuration operations	
Delete	You cannot delete dynamically created objects. A RADIUS CoA message must request their deletion, or the control channel for the dynamic service that created the object must be disconnected.
Create child objects	You cannot create objects within dynamically created sites; for example, subscriber interfaces or spoke SDP bindings.
Topology map actions	You cannot interact with dynamically-created objects that appear on the service topology map, except to display their parameters.
SAP copy/move	Dynamically created SAPs are not included in SAP copy or move operations. The operations proceed normally, but skip any dynamically created SAPs.
MDA or card removal	You cannot delete MDAs or cards with dynamic sites.
Automated operations	
Automatic MEP/MIP creation	MEGs skip MEP or MIP creation on SAPs and SDP bindings that are on a dynamically-created site.
SDP binding auto-completion	Dynamically-created sites are skipped during SDP binding auto-completion.
Service Throughput site list	Dynamically-created sites do not appear on the Service Throughput form

ID range behavior

Each NE that is configured for dynamic service must specify an ID range for dynamically-created sites. Dynamically-created sites can only use IDs from the specified range, and non-dynamic sites cannot use IDs from that range. When a dynamic service is created on an NE, the next available ID from the specified range is used.

75.3 Workflow to create dynamic services

The following workflow lists the high-level steps required to configure an NE to process dynamic service requests. As a prerequisite for creating a dynamic service, this workflow assumes that the following appropriate preconfigurations have been performed:

- pre-discovery CLI modifications
- discovery including mediation configuration with CLI user name and password
- creation of python scripts to be called by the NE; for more information about creating dynamic service python scripts, and CLI operations supported for python scripts, see the *7750 SR OS Triple Play Guide*.
- creation of RADIUS policies

1. Create a RADIUS script policy; see Procedure 54-16.
2. Create a dynamic service policy; see Procedure 75-1.
3. Configure the NE for dynamic service; see Procedure 75-2.
4. Configure a RADIUS-authenticated control channel. See the *7750 SR OS Triple Play Guide* for more information about dynamic service control channels.
5. If required, list the dynamically created objects on an NE; see Procedure 75-3.
6. If required, delete a dynamic service and all associated dynamically-created objects by deleting the control channel.

75.4 Dynamic service management procedures

Use the following procedures to perform dynamic service creation and management tasks.

Procedure 75-1 To configure a dynamic service policy

1 Choose Policies→Dynamic Service Policy from the 5620 SAM main menu. The Dynamic Service Policy form opens.

2 Perform one of the following:

a Create a dynamic service policy

i Click on the Create button. The Dynamic Service Policy, Global Policy (Create) form opens with the General tab displayed.

ii Go to step 3.

b Modify an existing dynamic service policy.

i Configure the filter criteria and click on the Search button. A list of dynamic service policies appears.

ii Select a dynamic service policy and click on the Properties button. The Dynamic Service Policy (Edit) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- SAP Limit

4 Click on the Select button beside the Script Policy parameter and select a RADIUS script policy for the dynamic service policy. See Procedure 54-16 for information about configuring RADIUS script policies.

5 Click on the Select button beside the CLI User parameter and select a CLI user for the dynamic service policy.

6 Click on the Accounting tab. Each dynamic services policy has two accounting instances.

7 Choose an accounting instance and click on the Properties button. The Accounting (Create) form appears.

8 Configure the parameters:

- Instance
- Stats Type

9 Click on the Select button beside the RADIUS Server Policy parameter and select a RADIUS server policy for the accounting instance. See Procedure 49-4 for information about configuring RADIUS server policies.

10 Configure the parameters in the Update Interval panel:

- Hours
- Minutes
- Days
- Disable Update Interval
- Update Interval Jitter
- Set Jitter to 10% of Update Interval

11 Click on the OK button. If required, repeat steps 7 to 11 for the other accounting instance. The Accounting (Create) form closes.

12 On the Dynamic Service Policy (Create) form, click on the OK button. The Dynamic Service Policy form closes.

13 On the Dynamic Service Policy list form, click on the Search button to display the newly created policy or policies. Choose a policy.

14 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.



Note — When the policy is in draft mode, the Distribute button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 42 for more information.

Procedure 75-2 To configure an NE for dynamic service

1 Choose Manage→Service→Dynamic Service NE Configuration from the 5620 SAM main menu. The Dynamic Service NE Configuration form appears.

2 Configure the filters and click on the Search button. A list of NEs that support dynamic services appears.

3 Choose an NE and click on the Properties button. The Dynamic Service NE Configuration (Edit) form appears.

4 Disable the Disable Creation parameter to allow the dynamic creation of network objects on the NE.

5 Define an ID range using the Start and End parameters. Dynamically-created objects are created using IDs from within the specified range.

6 Configure the Access-Accept parameter in the Timers panel.

7 Click on the OK button. The Dynamic Service NE Configuration (Edit) form closes.

Procedure 75-3 To list dynamically created objects on an NE

1 Choose Manage→Service→Dynamic Service NE Configuration from the 5620 SAM main menu. The Dynamic Service NE Configuration form appears.

2 Configure the filters and click on the Search button. A list of NEs that support dynamic services appears.

3 Choose an NE and click on the Properties button. The Dynamic Service NE Configuration (Edit) form appears.

4 Click on one of the following tabs to list the related dynamically created objects on the NE:

- Dynamic SAP Info
- Root Objects
- Script Snippets
- Service Sites

5 Click on the Search button to query the NE. A list of dynamically created objects appears.



Note — The list of objects in the Dynamic SAP Info tab is automatically updated.

6 Click on the OK button. The Dynamic Service NE Configuration (Edit) form closes.

76 — Application assurance

76.1 Application assurance overview *76-2*

76.2 ISA-AA groups and partitions *76-4*

76.3 AA components *76-6*

76.4 5670 RAM reporting attributes *76-11*

76.5 AA accounting policies *76-13*

76.6 Workflow to configure AA *76-14*

76.7 Application assurance procedures *76-15*

76.1 Application assurance overview

Application Assurance, or AA, is a service-enabling technology that enhances the hierarchical per-subscriber, per-service, and per-application QoS functions by providing more granular traffic control. In addition to QoS enhancements, AA provides traffic diversion, application identification, statistics collection, and data reporting to the 5670 RAM.

AA enables deep packet inspection of subscriber traffic where policies are applied to specific traffic types on a per-subscriber basis to determine the action to perform on the traffic.

AA and dynamic subscriber policy control allow a broadband network to provide application-based subscriber management for Internet access. The benefits of AA for residential and business service providers are:

- enhanced application-level SLAs through policy-based network traffic control and improved QoS sophistication at the application and site level
- traffic flow thresholds and threshold-crossing notification
- application-aware reporting and performance analysis
- greater network security
- scalability to support a large number of services, and flexibility to control network costs

The 5620 SAM supports 7450 ESS, 7750 MG, and 7750 SR AA functions.



Note — AA is not supported on a single-slot chassis.

NE traffic is selected to be processed by AA and then undergoes inspection by an ISA-AA MDA. See chapter 14 for information about using the 5620 SAM to configure an ISA-AA group that contains one or more ISA-AA MDAs.

You can configure cflowd on an ISA-AA group. AA cflowd supports basic cflowd sampling, as well as TCP performance data collection for AA applications and application groups. Each ISA-AA group supports one cflowd instance. See chapter 14 for information about configuring AA cflowd on an ISA-AA group.



Note — AA policies can only be configured on an NE when an ISA-AA group is already configured on the system.

The two elements of AA processing are:

- identification of the traffic on a per-flow or per-session basis
- policy treatment of the identified traffic

AA protocol signatures

The 5620 SAM generates a set of signatures that identify AA protocols. The signature set includes:

- protocol support summary—list of protocols that can be identified with the load using a combination of pattern and behavioral techniques. The protocols are used to generate statistics by protocol and as input in combination with other information to identify applications.
- pattern signatures—set of pattern-match signatures used in analysis
- behavior signatures—set of diagnostic techniques used in analysis

Because protocol signatures are intended to be the most basic block of application identification, other AA components, such as application filters, are provided to further customize protocol signatures. Customization reduces the need for a new protocol signature load when a new application may need to be identified.

Each protocol can be referenced in the definition of one or more applications by the application filter definition. The assignment of each supported protocol to an application filter or application is optional, allowing for the addition of new signature protocols without the need to update the application filter and applications.

Protocol signature upgrades

The 5620 SAM supports signature upgrades without automatically affecting policy behavior. All post-R1 new signatures are disabled, by default, during an upgrade to ensure that policies or services are not affected.

You can obtain new protocol signatures by dynamically upgrading only the ISA-AA MDA software on an NE, if the new software is from the same major release. If the software is from a different major release, you must upgrade the entire NE to obtain the new signatures. See "Managing NE software upgrades" in the *5620 SAM System Administrator Guide* for information about performing device software upgrades.

The protocols that are included in R1 of a release are designated as parent signatures and cannot be disabled. Within a major release, all protocols introduced after R1 of a release as part of an isa-aa.tim ISSU are, by default, shut down. When shut down, protocols introduced after R1 do not change AA behavior. For example, traffic maps to the parent protocol on which the new signature is based. Enabling or disabling a new protocol takes affect for new flows only. The protocols must be enabled on a per-protocol basis to take effect. Perform Procedure 76-26 to enable AA protocols.

AA policers

AA policers can be bandwidth or flow limiting, and can have one of the following scopes:

- system scope—limits all traffic entering the ISA-AA MDA
- subscriber scope—limits apply to the traffic of a subscriber

After a policer is referred to by an AQP for one traffic direction, the same policer cannot be referred to in the other direction. AQP rules with policer actions must specify a traffic direction other than "both".

AA flow watermark policies

AA supports the configuration of high and low thresholds, or watermarks, for logs and traps when there is a high consumption of the flow table. The flow table has a limited size and the thresholds are established to alert users that the flow table is approaching maximum capacity. When the high threshold is reached, an alarm is generated. The alarm is cleared when the flow table capacity has dropped below the specified low threshold.

AA transit IP and transit prefix policies

AA transit IP and transit prefix policies define how AA transit subscribers are created by an NE. Transit IP policies can be configured to discover dynamic transit subscribers via DHCP or RADIUS, and can also be configured with a list of static transit subscribers. Transit IP policies can also be configured to discover dynamic transit subscribers when traffic is detected on a parent SAP or spoke SDP binding.

Transit prefix policies allow you to specify transit subscribers by using network or subscriber IP ranges.

AA transit subscribers can persist in the 5620 SAM database. Transit subscriber aggregators allow you to aggregate multiple database persisted transit subscriber instances for VPN sites.

Application performance reporting

Application performance reporting adds a layer of route configuration to the handling of AA TCP performance, RTP/UDP performance, and flow-based volume reporting to the 5670 RAM. You can enable application performance reporting on service objects, and configure default DCP groups with address rules to apply a DCP subnet group to an entire network, an IP address range, or a single IP address for Internet or intranet traffic.

You can also create custom DCP subnet groups and bind them to individual L3 access interfaces and spoke SDP bindings. The 5670 RAM ignores application performance reporting configuration and objects on services that do not have an associated application profile.

AA HTTP error redirect policies

AA HTTP error redirect policies allow you to specify templates for local NE termination of HTTP errors and web browser redirection to customized error pages according to HTTP error codes.

76.2 ISA-AA groups and partitions

The 5620 SAM supports ISA-AA partitions. An ISA-AA partition is a unique child object of an ISA-AA group that can be assigned its own AA policy. There is no relationship between partitions of different ISA-AA groups. You can partition an ISA-AA group into AA policy partitions with one partition for each VPN-specific AA service. The partition supports VPN-specific custom protocols, applications, application group definitions, policy definitions and reporting. Each partition policy can be divided into multiple application QoS policies using ASOs. Multiple ISA-AA groups are used to scale the number of VPN-specific AA policies.

Multiple ISA-AA groups

The following operations can be performed at the ISA-AA group level

- Define one or more ISA-AA groups to allow AA resource partitioning and reservation of different types of AA service.
- Assign physical ISA-AAs to a group.
- Specify forwarding classes to be diverted for inspection by the AA subscribers that belong to the group and choose the AA policy to be applied to the group.
- Configure redundancy and bypass mode features to protect against equipment failure.
- Configure QoS on IOMs that host ISA-AA traffic.
- Configure ISA capacity planning using low and high thresholds.
- Enable ISA-AA partitions for ISA-AA groups.

Residential services are an example where all AA services can be configured as part of a single group that encompasses all ISA-AAs. The configuration provides the management of common applications and reporting for all subscribers and services, with common or per-customer AQP (uses ASO characteristics to divide the AQP of the ISA-AA into per-application profile QoS policies).

Multiple ISA-AA groups can also be used to create separate services based on different sets of common applications, traffic diversion needs, or different redundancy models. Multiple ISA-AA groups can be used for:

- a mix of residential and business customers
- different business VPN verticals
- business services with a common template base but different levels of redundancy, forwarding class diversion, or scaling over what is supported per single group

ISA-AA partitions

ISA-AA groups and partitions improve the scaling of policies. If partitions are not configured, the ISA-AA group acts as a single partition. When partitions are configured, application identification, and policy and statistics configuration apply only to the partition and not any other partitions that are configured under the same AA group. Although the definition of application profiles and related ASO characteristics is in the context of a partition, the application profile names must be unique for the NE. Definition of applications, application groups, and AQPs are also specific and only apply to a specific partition.

The following operations can be performed at the ISA-AA partition level

- Define unique applications and application groups per partition.
- Define AQP policies per partition.
- Define common applications and application groups with per partition processing and accounting.

ISA-AA partitions support accounting and customized reporting for every AA subscriber associated with a partition. You can perform the following operations:

- Define different types of reporting and accounting policies for different partitions in a single AA group.
- Display AA group level protocol statistics with partition visibility (for example, you can view protocol counts that are reported for each partition of the group).

When you create or delete an ISA-AA partition, a default AA accounting policy is automatically created in or deleted from the ISA-AA partition. See Procedure 14-2 for information about how to create and configure ISA-AA groups and partitions.

76.3 AA components

The 5620 SAM supports AA component creation and configuration using configuration forms and scripts. Figure 76-1 shows the AA components.

Figure 76-1 AA components

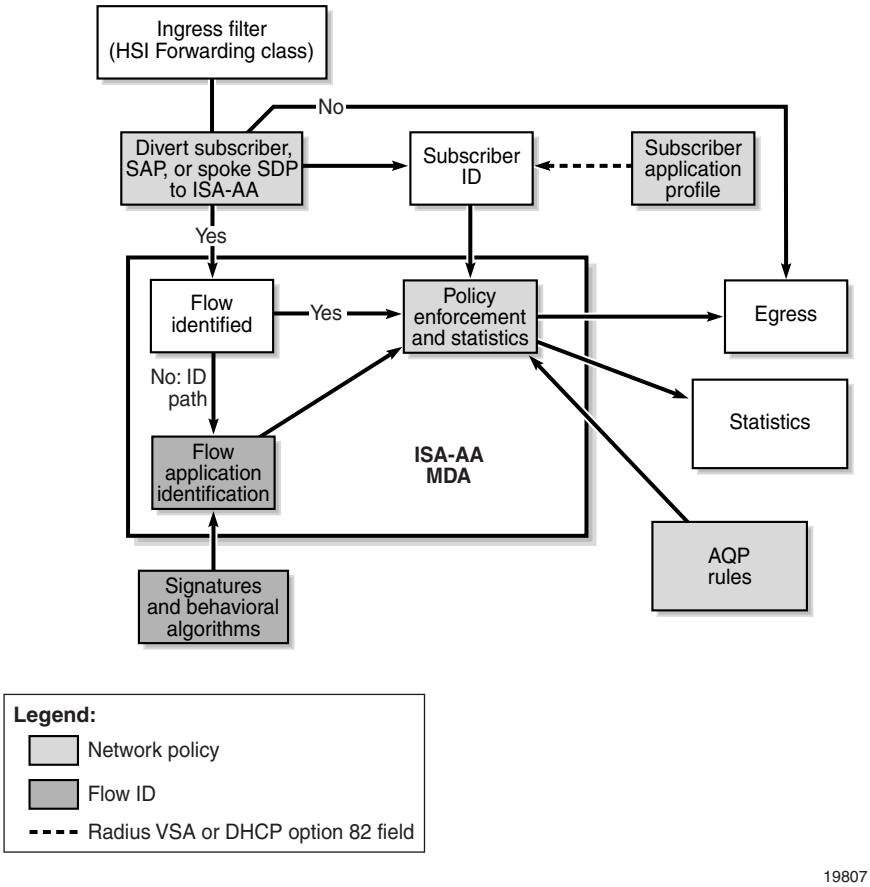
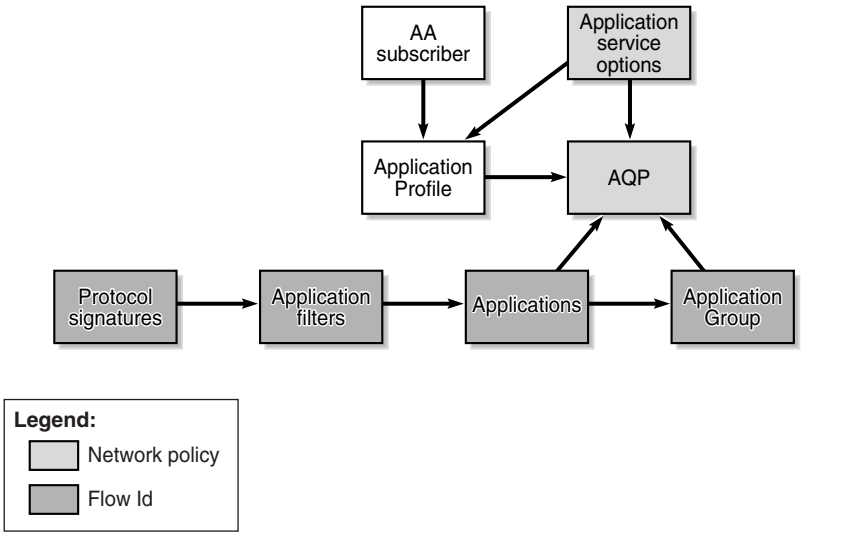


Figure 76-2 shows the relationship between the AA components.

Figure 76-2 AA policy structure



AA group policies

An AA group policy includes the following components:

- applications
- application groups
- application profiles
- application filters
- application service options, or ASOs
- application QoS policies, or AQPs
- custom protocols

Policy sync groups

Policy sync groups allow AA group policy components to be centrally defined and used across multiple ISA-AA groups and partitions. Policy sync groups define common AA group policy components by specifying a group policy as the master policy. The AA group policy classes of the master AA group are available to other AA groups that are members of the same policy sync group.

The list of AA group policy classes can be edited at the policy sync group level, with the option to include or exclude individual child classes. All actions for a given policy sync group affect only the child classes that are included for that policy sync group.

Use the Policy Sync Group menu option to designate an AA group policy as the master policy, and add one or more AA group policies as Policy Sync Group members. You can overwrite or add the contents of the master policy to one or more of its members.

Applications

Applications define and assign a description to the application names that are supported by the application filter entries. Each application is associated with one of the application groups. Applications are used by AA to identify the type of IP traffic in the subscriber traffic.

The application name is a key match criterion within the AQP rules that are applied to the IP traffic of a subscriber. The application name is also the unique identifier of the application object for northbound reporting systems such as the 5670 RAM. Changing an application name results in the loss of the previous application and the creation of a new application.

One predefined application ("unknown") is provided by AA. The unknown application cannot be modified. All other applications must be configured. An application must be configured before the associated application filter is defined.

Network operators can:

- change the application group that an application is associated with
- view which application filters are defining the application

You can obtain a CLI script from Alcatel-Lucent that updates the AA application database on an NE. Using the 5620 SAM script management function, you can update the list of applications on multiple NEs at one time. Contact Alcatel-Lucent technical support for more information.

Application groups

An application group is a container for multiple applications. A set of default application groups is provided by AA. At least one default application group ("unknown") must be associated with each NE. The default application groups cannot be modified.

Multiple applications can be assigned to an application group. An application can only belong to one group. Applications that are not assigned to an application group are automatically placed in the "unknown" application group.

Application profiles

Application profiles enable AA service for traffic to and from an ESM subscriber, SAP, or spoke SDP. Each application profile is unique and defines the AA service that the AA subscriber receives. The type of traffic is configured in the system-wide configuration of QoS forwarding classes to be diverted to the ISA-AA MDA for subscribers with AA enabled. The forwarding class is used for any subscriber traffic that a service provider needs to inspect using AA.

A subscriber can be assigned to an application profile that affects every host of the subscriber. For SAP or spoke SDP AA subscribers, an application profile can be assigned that affects the traffic originating from or destined for the SAP or spoke SDP.

For subscribers with application profiles that enable AA, traffic is diverted to the active ISA-AA MDA using ingress QoS policy filters. The filters identify forwarding and sub-forwarding classes that can be diverted for AA. The system identifies and diverts only traffic for any subscriber who is treated by the ISA-AA MDA, according to the application profile of the subscriber. Diversion to the ISA-AA MDA depends on the ISA-AA MDA status. If a subscriber is not configured to divert traffic to the ISA-AA MDA, normal ingress forwarding occurs.

The characteristics of application profiles are:

- By default, subscribers are not assigned to an application profile and traffic is not diverted for AA analysis.
- One or more application profiles can be configured.
- Application profiles are customer-defined and created using the configured application service options characteristics.
- Application profiles allow ASO characteristics to be associated with AA subscribers.
- Local instances of the application profile are configured to bind to specific objects of an NE (for example, L2 access interface, SAP, local subscriber explicit map entry, and so on).
- Application profiles can only be assigned when ISA-AA cards are assigned to an ISA-AA group
- Global application profiles must be manually distributed to the NEs.
- Application profiles can be assigned a capacity cost for subscriber load balancing among ISAs within the AA group.

ASOs

Application service options, or ASOs define the service provider and customer network functions that are common to sets of subscribers. ASOs prevent subscribers from requiring each subscriber-specific entry in the application QoS policies for standard network services.

In a typical application, ASOs define the HSI service parameters.

- ASOs are optional; AA can check the subscriber IP traffic without the use of application service options.
- ASOs can be configured for each AA group policy.
- ASOs are a series of user-defined application characteristics.
- ASO characteristics are used to create application profiles and provide information to user-defined AQP rules.
- The set of ASOs represent network-wide menus of service capabilities that are available to subscribers.

Some examples of ASOs are:

- entry for each managed application group; for example, VoIP, P2P, and HTTP
- multiple entries where specific applications in an application group can be individually managed as service parameters; for example, HTTP content from a specific content provider, or streaming video from network television or games

- HSI tiers, for example, Gold, Silver, and Bronze, that specify bandwidth levels
- bandwidth parameters for each service option

ASO characteristics are used:

- as input to application profiles
- by application QoS policies to influence how specific traffic is checked and how policies are applied

ASOs are assigned one or more characteristic values to define m service offerings to customers.



Caution — The 5620 SAM cannot discover or synchronize an ASO characteristic on an NE, or an object that references the ASO characteristic, if the characteristic name includes a forward slash (/).

During GUI- or OSS-based ASO configuration, the 5620 SAM prevents the inclusion of a forward slash in the Displayed Name value.

You can configure ASO characteristics for an AA subscriber using an AA subscriber policy override. An AA subscriber policy override can be configured for a SAP or spoke SDP binding, but not for an ESM subscriber. The AA subscriber must have an application profile assigned, or the subscriber policy override is rejected.

You can retrieve on demand the ASO values that are assigned to an AA subscriber from the Edit form of the SAP or spoke SDP binding AA subscriber.

Application filters

Application filters are provided as an indirect action between protocols and applications to allow the addition of variable parameters, for example, port numbers and IP addresses, to an application definition. An application filter contains numbered entries that define the use of protocol signatures and other application criteria. Multiple filter entries can be used to define an application, but each application filter entry maps to one application.

A traffic flow may have multiple filter entries. The entries are applied to the flow sequentially, and the matching entry with the lowest ID value is applied first. A traffic flow can be assigned to only one application.

You can accommodate the insertion of new entries in a list of entries by renumbering one or more of the existing entries using a GUI or OSS client. See Procedure 76-4 for information about renumbering application filter entries using the GUI.

AQPs

Application Qos Policies, or AQPs, are lists of rules that define the match criteria and action to be performed on all traffic flows. The AQP rules use the application groups, applications, and so on, as the match criteria. The output of the AQP rules defines the policy actions to perform.

AQP rules consist of match and action criteria:

- Match—Refers to the criteria used to identify a flow in order to apply actions such as dropping, forwarding, mirroring, and policing of bandwidth and flow. Matches cannot be made against protocols. Match criteria can be a combination of the following:
  - applications or application groups
  - ASO characteristics
  - flow direction
  - AA subscribers
  - flow source or destination IP address and/or port
- Action—Defines AA actions to be applied to traffic. For example, you can apply a set of actions such as bandwidth policing, packet discards, QoS remarking, and flow count, and/or rate limiting to a flow.

Custom protocols

Custom protocols are supported using configurable strings of up to 16 hexadecimal octets for pattern-matched application identification in the payload of TCP- and UDP-based applications. The match applies to the client-to-server, server-to-client, or any direction for TCP based applications, and to any direction for UDP-based applications.

You can configure a custom protocol description, custom protocol ID and shutdown. When a custom protocol is administratively disabled, traffic is identified as though the protocol is not configured.

Custom protocols and Alcatel-Lucent protocols are distinct; the span of a custom protocol is limited to the group or partition associated with an AA policy. Alcatel-Lucent protocols span all groups and partitions. Custom protocols are used in the application definition without limitations. All application filter entries, except strings, are supported. Custom protocol statistics collection on an ISA-AA partition group or special study subscriber is supported.

76.4 5670 RAM reporting attributes

5670 RAM reporting attributes are metadata parameters that specify how data is reported to the 5670 RAM. The parameters are not deployed to devices. Reporting attributes are configurable on the 5670 RAM Parameters tab of the AA application and AA application group properties form, and on the Application Assurance tab of the following properties forms:

- residential subscriber instance
- service
- SAP
- customer

The Reporting child tab contains service class and bandwidth reporting attributes that are configurable for the following objects:

- spoke SDP bindings
- access interfaces
- VPN-type transit prefix subscribers



Note — You must associate an application profile with an object before you can configure AA reporting for the object.

You can configure service-level IP detail reporting, which collects information about the top end users, by volume, of applications and applications groups. The following service types support IP detail configuration:

- IES
- VLL Epipe
- VLL Ipipe
- VPLS
- VPRN

Usage-based billing

The 5620 SAM supports application-specific reporting to the 5670 RAM based on configurable charging groups. You create charging groups as child objects of an AA group policy and can assign them to the following:

- applications
- application groups
- charging group thresholds
- AA subscriber statistics objects

You can assign one charging group to multiple applications or application groups, and can associate an application or application group with only one charging group.

You can configure charging groups with specific usage quotas and notification thresholds, and assign the thresholds to application profiles.

Residential DCP groups

On AA partitions and unpartitioned AA groups, a 5620 SAM operator can configure residential DCP groups that specify how to summarize the collected data. The 5670 RAM uses the group specifications as an aggregation framework for analysis and reporting.

A residential DCP group organizes subscriber traffic based on an IP address range that represents a subscriber address range or the server address range of a content provider. Residential DCP groups can help customers understand traffic patterns like the following:

- the volume of application traffic delivered to a specific regional market, for product management or policy development
- the application performance in a specific regional market; for example, how streamed video that is external in origin affects the local video-on-demand service
- the source of continuous high-volume traffic that is external in origin

76.5 AA accounting policies

AA accounting statistics provide information about application use in a network. You can configure AA accounting to collect and report statistics when at least one ISA-AA MDA is active. The AA accounting statistics provide information about application use on a SAP or spoke SDP, or by a subscriber during a collection interval. The collected information can be viewed in graphical or tabular form using the 5620 SAM GUI, or sent to a module such as the 5670 RAM for reporting and trend analysis.

AA accounting collects statistics on traffic flows. The 5620 SAM can collect the following AA statistics types:

- AA application
- AA application group
- AA protocol
- AA subscriber protocol (special-study)
- AA subscriber application (special-study)
- AA subscriber custom record

AA uses the 5620 SAM and NE accounting statistics and logging capabilities to collect statistics. See “Statistics collection overview” in the *5620 SAM Statistics Management Guide* for general information about configuring and collecting accounting statistics. See Procedure 76-7 for information about configuring an AA accounting policy.

The 5620 SAM can be configured to generate statistics for each protocol and application for a specific subscriber. You can enable AA statistics collection on a specific NE for a subset of subscribers for detailed traffic monitoring. An NE can have one policy for each AA statistics type that is enabled.

The AA subscriber protocol and AA subscriber application statistics are special study statistics for detailed accounting statistics collection on a limited number of subscribers, SAPs, or spoke SDPs on an NE. The number of subscribers, SAPs, or spoke SDPs is limited to constrain the volume of generated statistics.

Special study statistics are enabled by adding subscribers, SAPs, or spoke SDPs to a list in an ISA-AA group on an NE for AA debugging purposes. When a subscriber is on a special study list, the ISA-AA creates one statistics record for each application and application group that is associated with the subscriber. When a SAP or spoke SDP is on a special-study list, the ISA-AA creates one statistics record for each

application, application group, and protocol flow on the SAP or spoke SDP. See Procedure 14-2 for information about configuring special study objects in an ISA-AA group.

An AA custom record subscriber accounting policy applies to all subscribers, SAPs and spoke SDPs in an ISA-AA group for a specified set of AA protocols, applications, and application groups. The policy enables statistics collection on only the specified objects, which limits the volume of collected data and the statistics collection processing load. For example, a 5620 SAM operator may require statistics for only three application groups and 10 applications. You can view and configure the AA statistics objects from the AA Subscriber Stats Objects tab on the properties form of an ISA-AA group.

76.6 Workflow to configure AA

1. Configure the required ISA-AA groups and partitions on NEs. See Procedure 14-2.
2. Configure AA group policies using Procedure 76-1. As required, configure the following components:
   - ASOs and ASO overrides
   - application profiles
   - application groups
   - charging groups
   - applications
   - application filters
   - custom protocols
3. Configure AA policers. See Procedure 76-3.
4. Configure AQPs for AA group policies. See Procedure 76-5.
5. Create a policy sync group. See Procedure 76-6.
6. Create an AA accounting policy to specify when statistics are collected from the ISA-AA MDA. See Procedure 76-7.
7. Configure an AA flow watermark policy. See Procedure 76-8.
8. Configure AA transit IP policies and transit prefix policies as required.
   - **i** Configure AA transit IP policies. See Procedure 76-9.
   - **ii** Configure AA transit prefix policies. See Procedure 76-10.
   - **iii** Configure database persisted transit subscriber aggregators. See Procedure 76-11.
   - **iv** Associate database persisted transit subscribers with aggregators. See Procedure 76-12.

v Configure reporting attributes for AA reporting on a database persisted transit subscriber. See Procedure 76-13.

vi As required, view the database persisted transit subscriber information. See Procedure 76-14.

9 Configure usage-based billing as required:

i Enable usage-based billing at the application profile level. See Procedure 76-15.

ii Associate applications with charging groups. See Procedure 76-16.

10 Configure application performance reporting on a service. See Procedure 76-17.

11 Create a custom DCP subnet group for application performance reporting on a service and related objects. See Procedure 76-19.

12 Configure AA HTTP error redirect policies. See Procedure 76-20.

13 Configure AA HTTP redirect policies. See Procedure 76-21.

14 Configure AA protocol signatures and enable inactive protocols, as required. See Procedure 76-26.

15 As required, view AA results:

a view AA summary information for subscribers, transit subscribers, SAPs, and spoke SDPs on ISA-AA MDAs; see Procedure 76-27 for more information

b view the AA special study statistics data for subscribers, transit subscribers, SAPs, or spoke SDPs on an ISA-AA MDA; see Procedure 76-29 for more information

c view application filter hit counts on local definitions of AA group policies; see Procedure 76-28 for more information

d view application filter hit counts on local definitions of AA group policies; see Procedure 76-30 for more information

16 As required, delete AA objects or records.

a Delete an AA application, application group, or custom protocol; see Procedure 76-31 for more information.

b Remove the record of an inactive AA transit subscriber from the 5620 SAM database; see Procedure 76-32 for more information.

76.7 Application assurance procedures

Use the following procedures to configure AA policies and parameters in the 5620 SAM.

Procedure 76-1 To configure an AA group policy

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Perform one of the following:

a Create a policy. Perform the following steps.

i Click on the Create button and choose Create AA Group Policy from the drop-down list. The AA Group Policy (Create) form opens.

ii Configure the parameters:

- Group ID
- Partition ID

iii Click on the Apply button. The form name changes to AA Group Policy (Edit), and additional tabs are displayed.

b Configure an existing policy. Perform the following steps.

i Click on the Search button. The AA group policies are listed.

ii Select an AA group policy in the list and click on the Properties button. The AA Group Policy (Edit) form opens with the General tab displayed.

3 Configure the Description parameter.

4 To specify a default charging group, click on the Select button and choose a charging group from the Select Default Charging Group form.

5 To create an application group, perform the following steps.



Note — You can also manage application groups using the right-click contextual menu options for the Application Groups object on the AA Identification Components tab.

i Click on the Application Groups tab.

ii Click on the Create button. The Application Group (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Displayed Name
- Description
- Export ID



Note — You must select the check box beside the Export ID parameter before you can configure the parameter.

iv Click on the Charging Group tab.

v Click on the Select button and choose a charging group from the Select Charging Group form.

vi Click on the 5670 RAM Parameters tab.

vii Configure the Traffic Type parameter.

viii Click on the OK button. A dialog box appears.

ix Click on the OK button. The AA Group Policy (Edit) form reappears.

6 Repeat step 5 to create an additional application group, if required.

7 To create a charging group, perform the following steps.

i Click on the Charging Groups tab.

ii Click on the Create button. The Charging Group (Create) form opens.

iii Configure the parameters:

- Displayed Name
- Description
- Export ID



Note — You must select the check box beside the Export ID parameter before you can configure the parameter.

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The AA Group Policy (Edit) form reappears.

8 Repeat step 7 to create an additional charging group, if required.

9 To create an application, perform the following steps.



Note — You can also manage applications using the right-click contextual menu options for the Applications object on the AA Identification Components tab.

i Click on the Applications tab.

ii Click on the Create button. The Application (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Displayed Name
- Description
- Export ID



Note — You must select the check box beside the Export ID parameter before you can configure the parameter.

iv Click on the Application Group tab.

v Click on the Select button and choose an application group from the Select Application Group form.

vi Click on the Charging Group tab.

vii Click on the Select button and choose a charging group from the Select Charging Group form.

viii Click on the 5670 RAM Parameters tab.



Note — The 5670 RAM can perform an application performance index analysis on an AA application. An application performance index configuration is not distributed to an NE as part of a policy distribution.

The 5670 RAM provides a comparative analysis of TCP and UDP application usage. For each application, you can specify whether the application is TCP or UDP. TCP or UDP data is not distributed to an NE as part of a policy distribution.

ix Configure the general parameters:

- Application Flag
- Traffic Type

x Configure the parameters in the Thresholds panel:

- Threshold Administrative State
- Round Trip Time Tolerated (milliseconds)
- Mean Total Delay Tolerated (milliseconds)
- Total Delay Standard Deviation Tolerated (milliseconds)
- Packet Loss Tolerated (%)
- Frustrated (milliseconds)
- Frustrated (milliseconds)
- Frustrated (milliseconds)
- Frustrated (%)

xi Click on the OK button. A dialog box appears.

xii Click on the OK button. The Application (Create) form closes and the AA Group Policy (Edit) form reappears.

10 Repeat step 9 to create an additional application, if required.

11 To create an application filter, perform the following steps.



Note — You can also manage application filters using the right-click contextual menu options for the Application Filters object on the AA Identification Components tab.

i Click on the Application Filters tab.

ii Click on the Create button. The Application Filter (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Entry ID
- Description
- Administrative State

iv Click on the General Properties tab.

v Configure the Flow Set-up Direction parameter.

vi Configure the parameters in the IP Protocol panel, as required.

- IP Protocol Operator
- IP Protocol Number

vii Configure the parameters in the Protocol panel, as required.

- Protocol Operator
- Protocol Type

viii Configure the parameters in the Server panel, as required.

- Server Address Operator
- Server Address
- Server Address Mask

ix Configure the parameters in the Server Port panel, as required.

- Server Port Operator
- Server Port Value Type
- Server Port/Low Value
- Server Port High Value
- Server Port First Packet Policy

x Click on the Select button in the Protocol panel and choose a protocol from the Select Protocol or Select Custom Protocol form, depending on the Protocol Type parameter setting.

xi Click on the Application tab.

xii Click on the Select button in the Application panel and choose an application from the Select Application form.

xiii Click on the Application Filter Expressions tab.

xiv Click on the Create button. The Application Filter Expression (Create) form opens.

xv Configure the parameters:

- Index
- Type
- Operator
- String

xvi Click on the OK button. A dialog box appears.

xvii Click on the OK button. The Application Filter Expression (Create) form closes and the expression information is listed on the Application Filter (Create) form.

xviii Repeat step 11 xiv to xvii to create an additional application filter expression, if required.



Note — You can create a maximum of three application filter expressions.

xix Click on the OK button. A dialog box appears.

xx Click on the OK button. The Application Filter (Create) form reappears.

12 Repeat step 11 to create an additional application filter, if required.

13 Click on the OK button. A dialog box appears.

14 Click on the OK button. The Application Filter (Create) form closes and the AA Group Policy (Edit) form reappears.

15 To create an ASO, perform the following steps.

i Click on the Application Service Options tab.

ii Click on the Create button. The Application Service Option (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Displayed Name
- ASO Characteristic Default Value



Note — The Displayed Name of an ASO cannot contain a forward slash (/) character.

iv Click on the Application Service Option Value Entries tab.

v Click on the Create button. The Application Service Option Value Entry (Create) form opens.

vi Configure the ASO Characteristic Value parameter.

vii Click on the OK button. A dialog box appears.

viii Click on the OK button. The Application Service Option Value Entry (Create) form closes and the entry information is listed on the Application Service Option (Create) form.

ix Repeat steps 15 v to viii to create an additional ASO value entry.

x Click on the OK button. A dialog box appears.

xi Click on the OK button. The Application Service Option (Create) form closes and the AA Group Policy (Edit) form reappears.

16 Repeat step 15 to create an additional ASO, if required.

17 To create an application profile, perform the following steps.

i Click on the Application Profiles tab.

ii Click on the Create button. The Application Profile (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Displayed Name
- Description
- Divert
- Capacity Cost

iv Click on the 5670 RAM Parameters tab.

v Configure the Billing Reset Date parameter.

vi Configure the parameters in the Apdex Thresholds panel.

- Unacceptable
- Poor
- Fair
- Good

vii Configure the parameters in the MOS Thresholds panel.

- Unacceptable
- Poor
- Fair
- Good

viii Click on the Charging Group Thresholds tab.

ix Click on the Create button. The Charging Group Thresholds (Create) form opens.

x Configure the parameters:

- Quota (GB)
- Description
- Administrative State
- High Threshold (%)
- Middle Threshold (%)
- Low Threshold (%)

xi Click on the Select button and choose a charging group from the Select Charging Group form.

xii Click on the OK button. A dialog box appears.

xiii Click on the OK button. The Charging Group Thresholds (Create) form closes and the thresholds entry is listed on the Application Profile (Create) form.

xiv Click on the Characteristics tab.

xv Click on the Create button. The Application Profile Characteristic (Create) form opens.

xvi Click on the Select button beside the ASO Characteristic parameter and select an ASO Characteristic from the Select Application Service Option form.

xvii Click on the Select button beside the ASO Characteristic Value parameter and select an ASO characteristic value from the Select Application Service Option Characteristic Value form.

xviii Click on the OK button. A dialog box appears.

xix Click on the OK button. The Application Profile Characteristic (Create) form closes and the entry is listed on the Application Profile (Create) form.

xx Repeat steps 17 xv to xix to create an additional application profile characteristic, if required.

xxi Click on the OK button. A dialog box appears.

xxii Click on the OK button. The AA Group Policy (Edit) form reappears.

18 Repeat step 17 to create an additional application profile, if required.

19 Create a custom protocol, if required.

i Click on the Custom Protocols tab.

ii Click on the Create button. The Custom Protocol (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Entry ID
- Description
- IP Protocol Number
- Administrative State

iv Click on the Custom Protocol Expressions tab.

v Click on the Create button. The Custom Protocol Expressions (Create) form opens.

vi Configure the parameters:

- Index
- Custom Protocol Expression Offset
- Custom Protocol Expression Direction
- Operator
- String

vii Click on the OK button. A dialog box appears.

viii Click on the OK button. The Custom Protocol Expression (Create) form closes and the expression is listed on the Custom Protocol (Create) form.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Custom Protocol Expressions (Create) form closes and the AA Group Policy (Edit) form reappears.

20 Click on the OK button. A dialog box appears.

21 Click on the Yes button. The AA Group Policy (Edit) form closes, and the Application Assurance Policies form reappears.

22 Close the Application Assurance Policies form.

Procedure 76-2 To configure AARP

Perform this procedure to create or modify an AARP instance on an NE.

1 Choose Manage→ISA Functions→ISA AA from the 5620 SAM main menu. The Manage ISA-AA form opens.

2 Perform one of the following:

a Create an AARP instance. Perform the following steps.

i Click on the Create button and choose Create AARP from the drop-down list. The Select Network Elements form opens.

ii Select an NE in the list and click on the OK button. The AARP (Create) form opens.

iii Configure the ID parameter.

iv Click on the Apply button. The form name changes to AARP (Edit), and additional tabs are displayed.

b Configure an existing AARP instance. Perform the following steps.

i Choose AARP (Application Assurance) from the object drop-down list.

ii Click on the Search button. The AARP instances are listed.

iii Select an AARP instance in the list and click on the Properties button. The AARP (Edit) form opens with the General tab displayed.

3 Configure the following parameters:

- Description
- Peer IP Address

4 Perform one of the following.

a If the endpoint is a SAP, perform the following steps.

i Set the Peer Endpoint Type parameter to SAP.

ii If the SAP has a name, use the Select button to choose the SAP. Otherwise, configure the following parameters:

- SAP Terminating Port
- SAP Encapsulation Type
- SAP Outer Encapsulation Value
- SAP Inner Encapsulation Value

The SAP Outer Encapsulation Value parameter is configurable when the SAP Encapsulation Type parameter is set to Dot1 Q:

The SAP Inner Encapsulation Value parameter is configurable when the SAP Encapsulation Type parameter is set to Q in Q:

b If the endpoint is a spoke SDP binding, perform the following steps.

i Set the Peer Endpoint Type parameter to Spoke SDP Binding.

ii If the spoke SDP binding has a name, use the Select button to choose the spoke SDP binding. Otherwise, configure the Spoke SDP Bind ID parameter.

5 Configure the remaining parameters:

- Administrative State
- Priority
- Master Select Mode

6 Click on the Apply button. A dialog box appears.

7 Click on the Yes button.

8 View the Operational Flag and Peer Operational Flag indicators to ensure that the configuration is correct; modify the configuration, if required.

9 Close the AARP (Edit) form.

10 Close the Manage ISA-AA form.

Procedure 76-3 To configure an AA policer

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Perform one of the following:

a Create a policer. Perform the following steps.

i Click on the Create button and choose Create AA Policer from the drop-down list. The AA Policer (Create) form opens.

ii Configure the parameters:

- ISA-AA Group ID
- Displayed Name
- Type
- Granularity



Note — The distribution of an AA policer to an NE fails if the ISA-AA group specified by the ISA-AA Group ID does not exist on the NE.

iii Click on the Apply button. The form name changes to AA Policer (Edit), and additional tabs are displayed.

b Configure an existing policer. Perform the following steps.

i Choose AA Policer (Application Assurance) from the object drop-down list.

ii Click on the Search button. The policies are listed.

iii Select a policer in the list and click on the Properties button. The AA Policer (Edit) form opens with the General tab displayed.

3 Configure the Description parameter:

4 Perform one of the following:

a If the Type parameter is set to Dual Bucket Bandwidth, configure the following parameters:

- MBS (KB)
- CBS (KB)
- PIR (Kbps)
- CIR (Kbps)
- PIR
- CIR

b If the Type parameter is set to Flow Count Limit, configure the following parameters:

- Action
- Flow Count (flows)

c If the Type parameter is set to Flow Rate Limit, configure the following parameters:

- Action
- MBS (flows)
- PIR (flows/s)
- PIR

d If the Type parameter is set to Single Bucket Bandwidth, configure the following parameters:

- Action
- MBS (KB)
- PIR (Kbps)
- PIR

5 To configure a time-of-day override for the policer, perform the following steps.

i Click on the TOD Overrides tab.

ii Click on the Create button. The AA Policer Override (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Index
- Description
- Administrative State
- MBS
- CBS (KB)
- PIR (Kbps)
- CUR (Kbps)

iv Click on the Frequency tab.

v Configure the parameters:

- Frequency
- Start Hour
- End Hour
- Start Minute
- End Minute
- Start Day
- End Day



Note — The End Day parameter is configurable when the Frequency parameter is set to Weekly.

vi Click on the OK button. A dialog box appears.

vii Click on the OK button. The AA Policer Override (Create) form closes, and the time-of-day override is listed on the AA Policer (Edit) form.

6 Click on the OK button. A dialog box appears.

7 Click on the OK button. The AA Policer (Edit) form closes.

8 Close the Application Assurance Policies form.

Procedure 76-4 To renumber application filter entries

Perform this procedure to assign new ID values to one or more application filter entries in an AA group policy.



Note — The 5620 SAM renumbers a filter entry ID only when the following are true.

- The new value is unused.
- The new value is less than or equal to the maximum allowed value.
- The renumbering does not change the filter order.

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Choose AA Group Policy (Application Assurance) from the object drop-down list and click on the Search button. A list of AA group policies is displayed.

3 Select a policy in the list and click on the Properties button. The AA Group Policy (Edit) form opens with the General tab displayed.

4 Click on the Application Filters tab. A list of application filter entries is displayed.

5 To renumber one filter entry, perform the following steps.

i Select the entry and click on the Renumber ID button. The Renumber Entry ID form opens.

ii Configure the New Entry ID parameter.

iii Click on the OK button. The Renumber Entry ID form closes and a dialog box appears.

iv Click on the Yes button. The 5620 SAM renumbers the entry.

6 To renumber multiple filter entries, perform the following steps.

i Select the lowest-numbered entry that you want to renumber and click on the Renumber IDs button. The Renumber Entry ID form opens.

ii Configure the following parameters:

- Start Entry ID
- End Entry ID



Note — An End Entry ID value of 0 specifies that there is no ending entry ID; the range of entry IDs to renumber extends to the highest-numbered entry in the list.

iii Perform one of the following.

- Select Add Factor to add an offset to each entry ID in the specified range.
- Select Multiply Factor to multiply the ID of the selected entry and each higher-numbered entry in the specified range by an offset.

iv Configure the Factor Value parameter by specifying the required addition or multiplication offset.

v Click on the OK button. The Renumber Entry ID form closes and a dialog box appears.

vi Click on the Yes button. The 5620 SAM renumbers the entries.

7 Close the AA Group Policy (Edit) form.

8 Close the Application Assurance Policies form.

Procedure 76-5 To configure an AQP

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Choose AA Group Policy (Application Assurance) from the object drop-down list and click on the Search button. A list of AA group policies is displayed.



Note — The 5620 SAM does not create local AA Group policies for each applicable managed NE. Instead, the local AA Group Policy is created/deleted when the ISA-AA group is created/deleted.

3 Select a policy in the list and click on the Properties button. The AA Group Policy (Edit) form opens with the General tab displayed.

4 Click on the Application QoS Entries tab.

5 Click on the Create button. The Application QoS Policy (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Entry ID
- Description
- Administrative State

7 Click on the Match Criteria tab.

8 Configure the Traffic Direction parameter.

9 To specify an application as a criterion, perform the following steps.

i Configure the Application Operator parameter.

ii Click on the Select button in the Application panel and choose an application from the Select Application Name - Application QoS Policy form.

10 To specify an application group as a criterion, perform the following steps.

i Configure the Application Group Operator parameter.

ii Click on the Select button in the Application Group panel and choose an application group from the Select Application Group Name - Application QoS Policy form.

11 To specify DSCP criteria, configure the parameters in the DSCP panel:

- DSCP Operator
- DSCP

12 To specify IP criteria, configure the parameters in the IP Protocol panel:

- IP Protocol Operator
- IP Protocol Number

13 To specify a charging group as a criterion, perform the following steps.

i Configure the Charging Group Operator parameter.

ii Click on the Select button in the Charging Group panel and choose a charging group from the Select Charging Group - Application QoS Policy form.

14 To configure subscriber criteria, click on the AA Subscriber tab. Otherwise, go to step 17.

15 Configure the Subscriber Type parameter.



Note 1 — The SAP and Spoke SDP Binding options for the Subscriber Type parameter are selectable only for local AQP entry creation.

Note 2 — If the Subscriber Type parameter is set to None, the other parameters on the AA Subscriber tab are reset to the default values.

16 Perform one of the following:

a If the SubscriberType parameter is set to ESM, configure the ESM Subscriber parameter.

b If the SubscriberType parameter is set to SAP, configure the SAP Subscriber parameter.

c If the SubscriberType parameter is set to Spoke SDP Binding, configure the Spoke Subscriber parameter.

d If the SubscriberType parameter is set to Transit, configure the Transit Subscriber parameter.

17 To configure source or destination criteria, perform the following steps.

i Click on the Source and Destination tab.

ii Configure the parameters in the Source Address panel:

- Address Operator
- Address
- Address Length

iii Configure the parameters in the Source Port panel:

- Port Operator
- Port Value Type
- Port Value/Low Value
- Port High Value

iv Configure the parameters in the Destination Address panel:

- Address Operator
- Address
- Address Length

v Configure the parameters in the Destination Port panel:

- Port Operator
- Port Value Type
- Port Value/Low Value
- Port High Value

18 To configure ASO characteristic criteria, perform the following steps.

i Click on the Characteristics tab.

ii Click on the Create button. The Application QoS Policy Characteristic (Create) form opens.

iii Configure the parameters:

- ASO Characteristic
- ASO Characteristic Operator
- ASO Characteristic Value

iv Click on the OK button. A dialog box appears.

v Click on the Yes button. The Application QoS Policy Characteristic (Create) form closes.

19 Click on the Action tab.

20 Configure the Drop parameter.

21 If you select the Drop parameter, go to step 31.

22 Click on the Select buttons in the following panels, as required, and use the form that opens to choose the associated agent:

- Bandwidth Limit Policer
- Flow Rate Limit Policer
- Flow Count Limit Policer
- HTTP Error Redirect

23 To configure HTTP redirect, perform the following steps.

i Click on the Select button in the HTTP Redirect panel and use the form that opens to choose an HTTP redirect policy.

ii Configure the Flow Type parameter.

24 Click on the Select button in the HTTP Enrichment panel and use the form that opens to choose an HTTP enrichment policy.

25 Click on the Select button in the HTTP Notification panel and use the form that opens to choose an HTTP notification policy.

26 Click on the Select button in the Session Filter panel and use the form that opens to choose a session filter.



Note — The following devices support AA session filters:

- 7750 MG, Release 4.0 R6 or later
- 7450 ESS, Release 11.0 or later
- 7750 SR, Release 11.0 or later

27 Configure the parameters:

- Subscriber Cut Through
- Mirror Source All Inclusive



Note — The Mirror Source All Inclusive parameter is configurable only when you configure an AQP entry in a local definition of the AA group policy.

28 Click on the Select button in the Mirror Source panel to choose a mirror service from the Select Mirror Service form.



Note — You can specify a mirror service only when you configure an AQP entry in a local definition of the AA group policy.

29 Click on the Select button in the URL Filter panel and use the form that opens to choose a URL filter.

30 Configure the remarking parameters in the Remark panel:

- Forwarding Class
- Priority
- Remark DSCP In Profile
- Remark DSCP Out Profile

31 Click on the OK button. A dialog box appears.

32 Click on the OK button. The Application QoS Policy (Create) form closes.

33 Close the AA Group Policy (Edit) form.

34 Close the Application Assurance Policies form.

Procedure 76-6 To configure a policy sync group

1 Choose Policies→Policy Sync Group from the 5620 SAM main menu. The Policy Sync Groups form opens.

2 Perform one of the following:

a Create a policy sync group. Perform the following steps.

i Click on the Create button and choose Policy Sync Group. The Policy Sync Group (Create) form opens.

ii Configure the parameters:

- ID
- Auto-Assign ID

iii Click on the Select button in the Master Policy panel to choose a master policy from the Select Master Policy - Policy Sync Group form.

iv Click on the Apply button. The Policy Sync Group (Create) form name changes to Policy Sync Group (Edit), and the form displays additional tabs.

b Configure an existing policy sync group. Perform the following steps.

i Click on the Search button. A list of policy sync groups is displayed.

ii Select a group in the list and click on the Properties button. The Policy Sync Group (Edit) form opens with the General tab displayed.

3 Configure the following parameters:

- Description
- Displayed Name

4 To specify the AA group policy classes to include in the policy sync group, perform the followings steps.

i Click on the Included Classes tab. The tab lists the classes that are included in the policy sync group.



Note — The Sync Members, Add to Members, and Update Master actions performed on an AA group policy affect only the classes listed under the Included Classes tab.

ii To add one or more classes, click on the Add button and use the Select form that opens to specify the classes. The classes are listed on the Policy Sync Group (Edit) form.

iii To delete one or more classes, select the classes and click on the Delete button. The classes are removed from the list.

5 To add a member AA group policy, perform the following steps.

i Click on the Members tab.

ii Click on the Add button. The Select AA Group Policy - Policy Sync Group form opens.

iii Choose one or more AA group policies in the list and click on the OK button. The Confirm form opens. The form displays the following options:

- Listed master policy classes will overwrite member classes
- Listed master policy classes will be added to member classes



Note 1 — The Sync Members button performs the same function as the "Listed master policy classes will overwrite member classes" option.

Note 2 — The Add to Members button performs the same function as the "Listed master policy classes will be added to member classes" option.

iv Choose an option and click on the OK button. The member is listed on the Policy Sync Group (Edit) form.

6 To remove a member AA group policy, perform the following steps.

i Click on the Members tab.

ii Select a member policy in the list.

iii Click on the Delete button. The member policy is removed from the list.

7 To compare two member policies, perform the following steps.

i Select two policies in the list and click on the Compare button. The Compare - AA Group Policy form opens.



Note — You can use the Swap button to switch Policy A and Policy B.

ii Click on the Compare button to view the differences between Policy A and Policy B.

iii Choose a result and click on the Properties button. The Difference - AA Group Policy (*class type*) form opens.

iv View the differences between the two policies.



Note — After a Sync Member or Add to Member action, the member policy mode changes to Draft.

8 To add the classes defined in the master policy to each member policy, click on the Add To Members button. The master policy classes are added to each member policy.

9 To synchronize each member policy with the master policy, click on the Sync Members button. The master policy class list overwrite the class list in each member policy.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The Policy Sync Group (Edit) form closes, and the Policy Sync Groups form reappears.

12 Close the Policy Sync Groups form.

Procedure 76-7 To configure an AA accounting policy

See "Statistics collection overview" in the *5620 SAM Statistics Management Guide* for general information about configuring and collecting accounting statistics.

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Perform one of the following:

a Create a policy. Perform the following steps.

i Click on the Create button and choose AA Accounting Policy. The AA Accounting Policy (Create) form opens.

ii Configure the parameters:

- Group ID
- Partition ID

iii Click on the Apply button. The form name changes to AA Accounting Policy (Edit), and additional tabs are displayed.

b Configure an existing policy. Perform the following steps.

i Choose AA Accounting Policy (Application Assurance) from the object drop-down list.

ii Click on the Search button. A list of AA accounting policies is displayed.

iii Select a policy in the list and click on the Properties button. The AA Accounting Policy (Edit) form opens.

3 Configure the Description parameter.

4 Click on the Apply button. The form displays additional tabs.

5 Click on the Accounting Policies tab. A list of accounting policies is displayed.

6 Configure each accounting policy in the list, if required.

i Select the accounting policy and click on the Properties button. The AA Accounting Configuration form is displayed.

ii Configure the parameters:

- Description
- Collect Accounting Statistics

iii Click on the Select button in the Accounting Policy panel to choose an accounting policy from the Select Accounting Policy form.

iv Configure the following policy-specific parameters, if required:

- Administrative State
- Collect Aggregate Statistics
- Collect Maximum Throughput Statistics
- TCP Retransmission Packets Exclusion



Note — The TCP Retransmission Packets Exclusion parameter is configurable only on a Release 4.0 R5 or later 7750 MG, and only when the accounting policy type is AA Subscriber Custom Record.

v Click on the OK button. The AA Accounting Configuration (Edit) form closes.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The AA Accounting Policy (Edit) form closes, and the Application Assurance Policies form reappears.

9 Close the Application Assurance Policies form.

Procedure 76-8 To configure an AA flow watermark

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Choose AA Flow Watermark (Application Assurance) from the object drop-down list.

3 Click on the Search button. The AA flow watermarks are listed.

4 Select an entry in the list and click on the Properties button. The AA Flow Watermark (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Flow Full High Watermark
- Flow Full Low Watermark
- Flow Setup High Watermark
- Flow Setup Low Watermark
- Packet Rate High Watermark
- Packet Rate Low Watermark
- Bit Rate High Watermark
- Bit Rate Low Watermark

6 Click on the Apply button. A dialog box appears.

7 Click on the Yes button. The Configuration Mode changes to Draft.

8 Click on the Switch Mode button. A dialog box appears.

9 Click on the Yes button. The Configuration Mode changes to Released.

10 Click on the Distribute button to manually distribute the policy to one or more NEs. The Distribute - AA Flow Watermark form opens.

11 Select one or more NEs in the Available Nodes panel to which you want to distribute the policy and click on the right arrow. The NEs move to the Selected Nodes panel.

12 Click on the Distribute button. The policy is distributed to the NEs.

13 Close the Distribute - AA Flow Watermark form. The Application Assurance Policies form reappears.

14 Close the Application Assurance Policies form.

Procedure 76-9 To configure an AA transit IP policy

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Perform one of the following.

a Create an AA transit IP policy. Perform the following steps.

i Click on the Create button and choose AA Transit IP Policy. The AA Transit IP Policy (Create) form opens with General tab displayed.

ii Configure the following parameters:

- Group ID
- Partition ID
- Auto-Assign ID
- Policy ID

b Configure an existing AA transit IP policy. Perform the following steps.

i Choose AA Transit IP Policy (Application Assurance) from the object drop-down list.

ii Click on the Search button. The AA transit IP policies are listed.

iii Select a policy in the list and click on the Properties button. The AA Transit IP Policy (Edit) form opens.

3 Configure the following parameters:

- Description
- IPv6 Address Prefix Length

4 Click on the Select button in the Default Application Profile panel to choose a default application profile from the Select Default Application Profile - AA Transit IP Policy form.



Note — Only application profiles with the same Group ID and Partition ID values as the AA transit IP policy are listed.

5 Click on the Select button in the Subscriber Identification Policy panel to choose a subscriber identification policy from the Select Subscriber Identification Policy form.

6 Configure the following parameters:

- DHCP
- Seen IP
- Auto Create
- RADIUS



Note — The following parameters cannot be enabled at the same time:

- DHCP, and RADIUS or Seen IP
- Auto Create, and DHCP or RADIUS

7 If the RADIUS parameter is set to Enabled, click on the Select button in the Subscriber Authentication Policy panel to choose a subscriber authentication policy from the Select Subscriber Authentication Policy form.

8 If the RADIUS parameter is set to Enabled, click on the Select button in the AA RADIUS Accounting Policy panel to choose an AA RADIUS accounting policy from the Select AA RADIUS Accounting Policy form.

9 To add a static subscriber to the policy, perform the following steps.

i Click on the Subscribers tab.

ii Click on the Create button. The Transit Subscriber (Create) form opens with the General tab displayed.

iii Configure the Displayed Name parameter.

iv Click on the Select button in the Application Profile panel to choose an application profile from the Select Application Profile form.

v Click on the IP Addresses tab.

vi Click on the Create button. The Transit IP Address (Create) form opens.

vii Configure the Address parameter.

viii Click on the OK button. The address is listed on the Transit Subscriber (Create) form.

ix Repeat steps vi to viii to add another address, if required.

x Click on the OK button. A dialog box appears.

xi Click on the OK button. The Transit Subscriber (Create) form closes.

10 Repeat step 9 to add another static subscriber to the AA transit IP policy, if required.

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The AA Transit IP Policy (Create) or (Edit) form closes and the Application Assurance Policies form reappears.

13 Close the Application Assurance Policies form.

Procedure 76-10 To configure an AA transit prefix policy

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Perform one of the following.

a Create an AA transit prefix policy. Perform the following steps.

i Click on the Create button and choose AA Transit Prefix Policy. The AA Transit Prefix Policy (Create) form opens with the General tab displayed.

ii Configure the parameters:

- Group ID
- Partition ID
- Auto-Assign ID
- Policy ID

iii Click on the Apply button. The form name changes to AA Transit Prefix Policy (Edit), and additional tabs are displayed.

b Configure an existing AA transit prefix policy. Perform the following steps.

i Choose AA Transit Prefix Policy (Application Assurance) from the object drop-down list.

ii Click on the Search button. The AA transit prefix policies are listed.

iii Select an AA transit prefix policy in the list and click on the Properties button. The AA Transit Prefix Policy (Edit) form opens with the General tab displayed.

3 Configure the Description parameter.

4 To configure a subscriber, perform the following steps.

i Click on the Subscribers tab.

ii Click on the Create button. The Transit Prefix Subscriber (Create) form opens.

iii Configure the parameters:

- Displayed Name
- Remote

iv Click on the Select button in the Application Profile panel to choose an application profile from the Select Application Profile - Transit Prefix Subscriber form.

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The Transit Prefix Subscriber (Create) form closes, and the subscriber is listed on the AA Transit Prefix Policy (Edit) form.

vii Repeat steps ii to vi to create an additional transit prefix subscriber, if required.

5 To create a transit prefix entry, perform the following steps.

i Click on the Entries tab.

ii Click on the Create button. The Transit Prefix Entry (Create) form opens.

iii Click on the Select button in the Subscriber panel to choose a subscriber from the Select Subscriber - Transit Prefix Entry form.

iv Configure the parameters:

- Match Subscriber Address
- Subscriber Address
- Match Network Address
- Network Address
- ID
- Auto-Assign ID
- Subscriber Address Prefix Length
- Network Address Prefix Length

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The Transit Prefix Entry (Create) form closes, and the entry is listed on the AA Transit Prefix Policy (Edit) form.

vii Repeat steps ii to vi to create an additional transit prefix entry, if required.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The AA Transit Prefix Policy (Edit) form closes and the Application Assurance Policies form reappears.

8 Close the Application Assurance Policies form.

Procedure 76-11 To configure a database persisted transit subscriber aggregator

1 Choose Manage→AA Transit Subscribers from the 5620 SAM main menu. The Manage AA Transit Subscribers form opens.

2 Perform one of the following:

- **a** Create a database persisted transit subscriber aggregator. Perform the following steps.
  - **i** Click on the Create button and choose Transit Subscriber Aggregator. The Database Persisted Transit Subscriber Aggregator (Create) form opens with the General tab displayed.
  - **ii** Configure the Name parameter.
  - **iii** Click on the Apply button. The form name changes to Database Persisted Transit Subscriber Aggregator (Edit), and additional tabs are displayed.
- **b** Configure an existing database persisted transit subscriber aggregator. Perform the following steps.
  - **i** Choose Database Persisted Transit Subscriber Aggregator (Application Assurance) from the object drop-down list.
  - **ii** Click on the Search button. The database persisted transit subscriber aggregators are listed.
  - **iii** Select a database persisted transit subscriber aggregator in the list and click on the Properties button. The Database Persisted Transit Subscriber Aggregator (Edit) form opens with the General tab displayed.

3 Configure the parameters:

- Description
- Keyword List

4 Click on the OK button. The Database Persisted Transit Subscriber Aggregator (Edit) form closes, and the Manage AA Transit Subscribers form reappears.

5 Close the Manage AA Transit Subscribers form.

Procedure 76-12 To associate a database persisted transit subscriber with an aggregator



Note — You can only associate an aggregator object with database persisted transit subscribers that belong to ISA-AA groups for which the Subscriber Scale parameter is set to VPN.

1 Choose Manage→AA Transit Subscribers from the 5620 SAM main menu. The Manage AA Transit Subscribers form opens.

2 Choose Database Persisted Transit Subscriber (Application Assurance) from the object drop-down list.

3 Click on the Search button. The database persisted transit subscribers are listed.

4 Select a database persisted transit subscriber in the list and click on the Properties button. The Database Persisted Transit Subscriber (Edit) form opens with the General tab displayed.

5 Click on the 5670 RAM Parameters tab.

6 Click on the Select button. The Select Database Persisted Transit Subscriber Aggregator form opens.

7 Configure the filter for the Keywords List column and click on the Search button. A list of database persisted transit subscriber aggregators is displayed.

8 Select an aggregator in the list and click on the OK button. The aggregator information is displayed on the Database Persisted Transit Subscriber (Edit) form.

9 Click on the OK button. A dialog box appears.

10 Click on the Yes button. The Database Persisted Transit Subscriber (Edit) form closes, and the Manage AA Transit Subscribers form reappears.

11 Repeat steps 4 to 10 to associate more database persisted transit subscribers with aggregators, as required.

12 Close the Manage AA Transit Subscribers form.

Procedure 76-13 To configure 5670 RAM AA reporting attributes for a database persisted transit subscriber



Note — You can perform this procedure only for VPN transit subscribers.

1 Choose Manage→AA Transit Subscribers from the 5620 SAM main menu. The Manage AA Transit Subscribers form opens.

2 Choose Database Persisted Transit Subscriber (Application Assurance) from the object drop-down list.

3 Configure the filter criteria, if required, and click on the Search button. A list of database persisted transit subscribers is displayed.

4 Select a subscriber in the list and click on the Properties button. The Database Persisted Transit Subscriber (Edit) form opens with the General tab displayed.

5 Click on the 5670 RAM Parameters tab.

6 Click on the Reporting tab.

7 Click on the Create button. The AA Reporting (Create) form opens.

8 Configure the parameters:

- Customer Name
- Subscriber Class
- Total Bandwidth Upstream (Kbps)
- Class of Service 1 Bandwidth Upstream (Kbps)
- Class of Service 2 Bandwidth Upstream (Kbps)
- Class of Service 3 Bandwidth Upstream (Kbps)
- Class of Service 4 Bandwidth Upstream (Kbps)
- Subscriber Name
- Subscriber Type
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)

9 Click on the OK button. The AA Reporting (Create) form closes and the reporting object is displayed in the list.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The Database Persisted Transit Subscriber (Edit) form closes, and the Manage AA Transit Subscribers form reappears.

12 Close the Manage AA Transit Subscribers form.

Procedure 76-14 To view database persisted transit subscriber information

1 Choose Manage→AA Transit Subscribers from the 5620 SAM main menu. The Manage AA Transit Subscribers form opens.

2 Choose Database Persisted Transit Subscriber (Application Assurance) from the object drop-down list.

3 Configure the filter criteria, if required, and click on the Search button. The database persisted transit subscribers are listed.

4 Select a subscriber in the list and click on the Properties button. The Database Persisted Transit Subscriber (Edit) form opens with the General tab displayed.

5 View the subscriber information, as required.

6 Close the Database Persisted Transit Subscriber (Edit) form.

7 Close the Manage AA Transit Subscribers form.

Procedure 76-15 To configure usage-based billing for an application profile

You must perform this procedure on an existing application profile. Perform Procedure 76-16 to assign applications to charging groups.

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Choose AA Group Policy (Application Assurance) from the object drop-down list.

3 Click on the Search button. The policies are listed.

4 Select an AA group policy in the list and click on the Properties button. The AA Group Policy form opens with the General tab displayed.

5 Click on the Application Profiles tab.

6 Select an application profile in the list and click on the Properties button. The Application Profile (Edit) form opens with the General tab displayed.

7 Click on the 5670 RAM Parameters tab.

8 Configure the Billing Reset Date parameter.

9 Configure the parameters in the Apdex Thresholds panel.

- Unacceptable
- Poor
- Fair
- Good

10 Configure the parameters in the MOS Thresholds panel.

- Unacceptable
- Poor
- Fair
- Good

11 Click on the Charging Group Thresholds tab.

12 Perform one of the following.

a Create a new charging group threshold set. Perform the following steps.

i Click on the Create button. The Charging Group Thresholds (Create) form opens.

ii Configure the parameters:

- ID
- Auto-Assign ID

b Configure an existing charging group threshold set. Select a charging group threshold in the list and click on the Properties button. The Charging Group Thresholds (Edit) form opens.

13 Configure the parameters:

- Quota (GB)
- Description
- Administrative State
- High Threshold (%)
- Middle Threshold (%)
- Low Threshold (%)

14 Click on the Select button and choose a charging group from the Select Charging Group form.

15 Click on the OK button. The Charging Group Thresholds (Edit) form closes.

16 Repeat steps 12 to 15 to configure an additional charging group, if required.

17 Click on the OK button. The Application Profile (Edit) form closes.

18 Click on the OK button. A dialog box appears.

19 Click on the Yes button. The AA Group Policy (Edit) form closes, and the Application Assurance Policies form reappears.

20 Close the Application Assurance Policies form.

Procedure 76-16 To associate an application with a charging group

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Choose AA Group Policy (Application Assurance) from the object drop-down list.

3 Click on the Search button. The AA group policies are listed.

4 Select an AA group policy in the list and click on the Properties button. The AA Group Policy (Edit) form opens with the General tab displayed.

5 Click on the Applications tab.

6 Select an application in the list and click on the Properties button. The Application (Edit) form opens with the General tab displayed.

7 Click on the Charging Group tab.

8 Click on the Select button to choose a charging group from the Select Charging Group form.

9 Click on the OK button. The Application (Edit) form closes.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The AA Group Policy (Edit) form closes, and the Application Assurance Policies form reappears.

12 Close the Application Assurance Policies form.

Procedure 76-17 To enable application performance reporting on a service using default DCP subnet groups

Perform this procedure to enable application performance reporting on a service and configure the default DCP subnet groups. See Procedure 76-19 for information about configuring custom DCP subnet groups.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria, if required, and click on the Search button. A list of services is displayed.

3 Select a service and click on the Properties button. The *service_type* Service (Edit) form opens with the General tab displayed.

4 Click on the 5670 RAM Parameters tab.

5 Select the Enable Application Performance Reporting parameter.

6 Click on the Apply button. A dialog box appears.

7 Click on the Yes button. The 5620 SAM creates default Internet and Intranet DCP subnet groups, which are listed on the Default DCP Groups tab.

8 To configure address rules for a default DCP subnet group, perform the following steps.

   i Click on the Default DCP Groups tab.

   ii Select a default subnet group in the list and click on the Properties form. The Default DCP Group (Edit) form opens with the General tab displayed.

   iii Click on the Address Rules tab.

   iv Click on the Create button. The DCP Address Rule (Create) form opens.

v Configure the parameters:

- Auto-Assign ID
- ID
- Description
- IP Address Low
- High
- Mask

vi Click on the OK button. A dialog box appears.

vii Click on the OK button. The DCP Address Rule (Create) form closes.

viii Repeat steps iv to vii to add another address rule, if required.

ix Click on the OK button. The Default DCP Group for closes.

9 Click on the OK button. A dialog box appears.

10 Click on the Yes button. The *service_type* Service (Edit) form closes, and the Manage Services form reappears.

11 Close the Manage Services form.

Procedure 76-18 To disable application performance reporting on a service

Perform this procedure to disable application performance reporting on a service and delete the default DCP subnet groups.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria, if required, and click on the Search button. A list of services is displayed.

3 Select a service and click on the Properties button. The *service_type* Service (Edit) form opens with the General tab displayed.

4 Click on the 5670 RAM Parameters tab.

5 Deselect the Enable Application Performance Reporting parameter.

6 Click on the Apply button. A dialog box appears.

7 Click on the Yes button.

8 Click on the Default DCP Groups tab.

9 Click on the Delete All Result button. A dialog box appears.

10 Click on the Yes button. The default DCP subnet groups are deleted.

11 Click on the OK button A dialog appears.

12 Click on the Yes button. The *service_type* Service (Edit) form closes, and the Manage Services form reappears.

13 Close the Manage Services form.

Procedure 76-19 To configure a custom DCP subnet group

Perform this procedure to create a custom DCP subnet group for application performance reporting on a service and child objects. A custom DCP subnet group must be bound to one or more access interfaces or spoke SDP bindings.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria, if required, and click on the Search button. A list of services is displayed.

3 Select a service and click on the Properties button. The *service_type* Service (Edit) form opens with the General tab displayed.

4 Click on the 5670 RAM Parameters tab.

5 Click on the Custom DCP Groups tab.

6 Click on the Create button. The Custom DCP Group (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Auto-Assign ID
- ID
- Description
- Address Type
- Collect Stats

8 To associate the subnet group with a SAP, click on the Select button in the SAP Subscriber panel and choose a SAP from the Select SAP Subscriber - Custom DCP Group form.

9 To associate the subnet group with a spoke SDP binding, click on the Select button in the spoke SDP binding Subscriber panel and choose a SAP from the Select Spoke SDP Binding Subscriber - Custom DCP Group form.

10 To associate the subnet group with a transit subscriber, click on the Select button in the spoke SDP binding Subscriber panel and choose a SAP from the Select Transit Subscriber - Custom DCP Group form.

11 To add an address rule to the subnet group, perform the following steps.

i Click on the Address Rules tab.

ii Click on the Create button. The DCP Address Rule (Create) form opens.

iii Configure the parameters:

- Auto-Assign ID
- ID
- Description
- IP Address Low
- High
- Mask

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The DCP Address Rule (Create) form closes.

vi Repeat steps ii to iv to add another address rule to the subnet group, if required.

12 Click on the OK button. A dialog box appears.

13 Click on the OK button. The Custom DCP Group (Create) form closes.

14 Click on the OK button. A dialog appears.

15 Click on the Yes button. The *service_type* Service form closes, and the Manage Services form reappears.

16 Close the Manage Services form.

Procedure 76-20 To configure an AA HTTP error redirect policy

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Choose one of the following:

a Create an AA HTTP error redirect policy. Perform the following steps.

i Click on the Create button and choose AA HTTP Error Redirect. The AA HHTP Error Redirect (Create) form opens with the General tab displayed.

ii Configure the parameters:

- ISA-AA Group ID
- Displayed Name

iii Click on the Apply button. The form name changes to AA HTTP Error Redirect (Edit), and the form displays additional tabs.

b Configure an existing AA HTTP error redirect policy. Perform the following steps.

i Choose AA HTTP Error Redirect (Application Assurance) from the object drop-down list.

ii Click on the Search button. The AA HTTP Error Redirect policies are listed.

iii Select an AA HTTP Error Redirect policy in the list and click on the Properties button. The AA HTTP Error Redirect (Edit) form opens with the General tab displayed.

3 Configure the parameters:

- Description
- Enabled
- HTTP Host
- Participant ID

4 Click on the Select button beside the Template ID parameter choose a template from the Select Template ID form. The template ID is displayed on the AA HTTP Error Redirect (Edit) form.

5 To configure an HTTP error code, perform the following steps.

i Click on the HTTP Error Codes tab.

ii Click on the Create button. The HTTP Redirect Error Code (Create) form opens.

iii Click on the Select button beside the Redirect Error Code parameter and choose an error code from the Select Error Code form. The error code is displayed on the HTTP Redirect Error Code (Create) form.

iv Configure the Message Size (octets) parameter.

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The HTTP Redirect Error Code (Create) form closes, and the error code is listed on the AA HTTP Error Redirect (Edit) form.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The AA HTTP Error Redirect (Edit) form closes, and the Application Assurance Policies form reappears.

8 Close the Application Assurance Policies form.

Procedure 76-21 To configure an AA HTTP redirect policy

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Choose one of the following:

a Create an AA HTTP redirect policy. Perform the following steps.

i Click on the Create button and choose AA HTTP Redirect. The AA HHTP Redirect (Create) form opens with the General tab displayed.

ii Configure the parameters:

- ISA-AA Group ID
- Displayed Name

iii Click on the Apply button. The form name changes to AA HTTP Redirect (Edit), and the form displays additional tabs.

b Configure an existing AA HTTP redirect policy. Perform the following steps.

i Choose AA HTTP Redirect (Application Assurance) from the object drop-down list.

ii Click on the Search button. The AA HTTP Redirect policies are listed.

iii Select an AA HTTP Redirect policy in the list and click on the Properties button. The AA HTTP Redirect (Edit) form opens with the General tab displayed.

3 Configure the parameters:

- Description
- Enabled
- HTTP Host

4 Click on the Select button beside the Template ID parameter choose a template from the Select Template ID form. The template ID is displayed on the AA HTTP Redirect (Edit) form.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The AA HTTP Redirect (Edit) form closes, and the Application Assurance Policies form reappears.

7 Close the Application Assurance Policies form.

Procedure 76-22 To configure an AA HTTP enrichment policy

Perform this procedure to create an AA HTTP enrichment policy that is to be associated with an AQP. See Procedure 76-5 for information about configuring an AQP.

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Perform one of the following:

a Create an AA HTTP enrichment policy. Perform the following steps.

i Click on the Create button and choose AA HTTP Enrichment. The AA HHTP Enrichment (Create) form opens with the General tab displayed.

ii Configure the parameters:

- ISA-AA Group ID
- Displayed Name

iii Click on the Apply button. The form displays additional tabs and panels.

b Modify an AA HTTP enrichment policy. Perform the following steps.

i Choose AA HTTP Enrichment (Application Assurance) from the object drop-down list.

ii Configure the filter criteria, if required, and click on the Search button. A list of AA HTTP enrichment policies is displayed.

iii Select a policy in the list and click on the Properties button. The AA HTTP Enrichment (Edit) form opens with the General tab displayed.

3 Configure the parameters:

- Description
- Enabled

4 Click on the HTTP Enrichment Fields tab.

5 Click on the Create button. The HTTP Enrichment Field (Create) form opens.

6 Perform one of the following.

a Click on the Select button and choose a field from the Select Field list form.

b Configure the Name parameter.

7 Configure the remaining parameters:

- Anti Spoof
- Encode Type
- Encode Key

The Anti Spoof parameter is configurable only on a Release 5.0 R5 or later 7750 MG.

The Encode Type and Encode Key parameters are configurable on a Release 11.0 R4 or later 7450 ESS or 7750 SR, and on a Release 5.0 R5 or later 7750 MG.

8 Repeat steps 5 to 7 to add another field, if required.

9 Click on the OK button. A dialog box appears.

10 Click on the OK button. The HTTP Enrichment Field (Create) form closes.

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The AA HTTP Enrichment (Edit) form closes and the Application Assurance Policies form reappears.

13 Close the Application Assurance Policies form.

Procedure 76-23 To configure an HTTP notification policy

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Perform one of the following:

a Create an AA HTTP notification policy. Perform the following steps.

i Click on the Create button and choose AA HTTP Notification. The AA HHTP Notification (Create) form opens with the General tab displayed.

ii Configure the parameters:

- ISA-AA Group ID
- Displayed Name

iii Click on the Apply button. The form name changes to AA HTTP Notification (Edit), and the form displays additional tabs.

b Configure an existing AA HTTP notification policy. Perform the following steps.

i Choose AA HTTP Notification (Application Assurance) from the object drop-down list.

ii Click on the Search button. The AA HTTP Notification policies are listed.

iii Select an AA HTTP Notification policy in the list and click on the Properties button. The AA HTTP Notification (Edit) form opens with the General tab displayed.

3 Configure the parameters:

- Description
- Administrative State
- Script URL
- Interval Type
- Interval (minutes)

The Interval (minutes) parameter is configurable when the Interval Type parameter is set to Minimum Interval.

4 Click on the Select button and use the form that opens to choose a template. The template ID is displayed on the AA HTTP Notification (Edit) form.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The AA HTTP Notification (Edit) form closes, and the Application Assurance Policies form reappears.

7 Close the Application Assurance Policies form.

Procedure 76-24 To configure an AA session filter

Perform this procedure to create an AA session filter that is to be associated with an AQP. See Procedure 76-5 for information about configuring an AQP.



Note — AA session filters are supported only by the following devices:

- 7750 MG, Release 4.0 R6 or later
- 7450 ESS, Release 11.0 or later
- 7750 SR, Release 11.0 or later

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Perform one of the following:

a Create an AA session filter. Perform the following steps.

i Click on the Create button and choose AA Session Filter. The AA Session Filter (Create) form opens with the General tab displayed.

ii Configure the parameters:

- Group ID
- Partition ID
- Displayed Name

iii Click on the Apply button. The form displays additional tabs and panels.

b Modify an AA session filter. Perform the following steps.

i Choose AA Session Filter (Application Assurance) from the object drop-down list.

ii Configure the filter criteria, if required, and click on the Search button. A list of AA session filters is displayed.

iii Select a filter in the list and click on the Properties button. The AA Session Filter (Edit) form opens with the General tab displayed.

3 Configure the parameters:

- Description
- Default Action

4 Click on the Entries tab.

5 Click on the Create button. The AA Session Filter Params (Create) form opens.

6 Configure the parameters:

- ID
- Description
- Action

7 Click on the Match Criteria tab.

8 Configure the Protocol Number parameter.

9 Configure the Source Address parameters:

- Source Address
- Length

10 Configure the Destination Address parameters:

- Destination Address
- Length

11 If the Protocol Number parameter is set to SCTP, TCP, or UDP, configure the following parameters in the Source Port and Destination Port panels, as required:

- Port Operator
- Port Value/Low Value
- Port High Value

12 Click on the OK button. A dialog box appears.

13 Click on the OK button. The AA Session Filter Params (Create) form closes.

14 Repeat steps 5 to 13 to add another filter entry, if required.

15 Click on the OK button. A dialog box appears.

16 Click on the Yes button. The AA Session Filter (Edit) form closes and the Application Assurance Policies form reappears.

17 Close the Application Assurance Policies form.

Procedure 76-25 To configure a URL filter

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Perform one of the following:

a Create a URL filter. Perform the following steps.

i Click on the Create button and choose URL Filter. The AA URL Filter (Create) form opens with the General tab displayed.

ii Configure the parameters:

- ISA-AA Group ID
- Displayed Name

iii Click on the Apply button. The form name changes to AA URL Filter (Edit), and the form displays additional tabs.

b Configure an existing URL filter. Perform the following steps.

i Choose AA URL Filter (Application Assurance) from the object drop-down list.

ii Click on the Search button. The AA URL filter policies are listed.

iii Select a URL filter in the list and click on the Properties button. The AA URL Filter (Edit) form opens with the General tab displayed.

3 Configure the parameters:

- Description
- Administrative State
- VLAN ID
- Default Action

4 If you set the Default Action parameter to Block Http Redirect, click on the Select button beside the HTTP Redirect Name parameter and use the form that opens to choose an HTTP Redirect policy.

5 Click on the Select button beside the ICAP HTTP Redirect Name parameter and use the form that opens to choose an HTTP Redirect policy.

6 To create an ICAP Server entry, perform the following steps.

i Click on the ICAP Server tab.

ii Click on the Create button. The AA ICAP Server Entries form opens.

iii Configure the parameters:

- Description
- Administrative State
- Server Address
- Server Port

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The AA URL Filter (Edit) form closes, and the Application Assurance Policies form reappears.

9 Close the Application Assurance Policies form.

Procedure 76-26 To enable an AA protocol signature

Perform this procedure to administratively enable an AA protocol signature for use by AA functions.

1 Choose Manage→ISA Functions→ISA-AA from the 5620 SAM main menu. The Manage ISA-AA form opens.

2 Choose AA Protocol (Application Assurance) from the object drop-down list.

3 Specify a filter to create a filtered list of protocols, and click on the Search button. A list of protocols is displayed.

4 Select an entry in the list and click on the Properties button. The AA Protocol (Edit) form opens.

5 View the entry information.

6 Configure the Protocol Administrative State parameter, if required.



Note — You can configure the Protocol Administrative State parameter only for a local protocol.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The AA Protocol (Edit) form closes, and the Manage ISA-AA form reappears.

9 Close the Manage ISA-AA form.

Procedure 76-27 To view AA summary information for an ISA-AA group or partition

Perform this procedure to view the AA summary information for an ISA-AA group or partition. You can view summary information for the following object types:

- subscribers
- transit subscribers

- SAPs
- spoke SDP bindings

AA summary information is typically used for AA debugging purposes. You can view debug statistics information on the Statistics tab of an AA object.



Caution — The AA summary information on the NE may be slightly out of synchronization with the 5620 SAM database. Before you attempt to resynchronize an ISA-AA group, Alcatel-Lucent recommends that you consider the effect of resynchronizing an ISA-AA group; such an operation may require the retrieval of a large volume of information, and may affect NE performance.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to an ISA-AA group. The path is Network→NE→Logical Groups→ISA-AA Group→ISA-AA Group.

3 Right-click on the ISA-AA Group icon and choose Properties from the contextual menu. The ISA-AA Group (Edit) form opens.

4 If partitions are enabled in the ISA-=AA group, perform the following steps.

i Click on the Partitions tab. The AA group partitions are displayed.

ii Select a partition in the list and click on the Properties button. The ISA-AA Group Partition (Edit) form opens.

5 To view the summary information for an object, perform the following steps.

i Click on the AA Summary tab. The following tabs are displayed; each tab lists the corresponding objects in the ISA-AA group:

- Subscribers
- SAPs
- Spoke SDP Bindings
- Transit Subscribers

ii Click on the appropriate tab.

iii Select an object in the list and click on the Properties button. The AA *object_type* (Edit) form opens.

iv View the information.

6 Close the open forms, as required.

Procedure 76-28 To view AA statistics data for an ISA-AA group or partition

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the required ISA-AA group. The path is Network→NE→Logical Groups→ISA-AA Groups-ISA-AA Group.

3 Right-click on the ISA-AA Group icon and choose Properties from the contextual menu. The ISA-AA Group (Edit) form opens with the General tab displayed.

4 Perform one of the following:

   a View AA statistics data for an ISA-AA group. Perform the following steps.

      i Click on the Statistics tab.

      ii Choose an AA statistics class from the object drop-down list.

   b View AA statistics data for an ISA-AA partition. Perform the following steps.

      i Click on the ISA-AA Partitions tab. A list of ISA-AA partitions is displayed.

      ii Select an entry in the list and click on the Properties button. The ISA-AA Group Partition (Edit) form opens with the General tab displayed.

      iii Click on the Statistics tab.

      iv Choose an AA statistics class from the object drop-down list.

5 Perform one of the following:

   a Click on the Collect button to perform an on-demand collection of the current performance statistics data. The collected statistics entries are listed on the form.

   b Click on the Collect All button to collect one on-demand statistics record for each statistic type that the object supports. The collected statistics entries are listed on the form.

6 Select an entry in the list and click on the Properties button. The Statistics Record form opens.

7 View the statistics data.

8 Close the Statistics Record form.

9 Close the AA *object_type* (Edit) form.

10 Close the ISA-AA Group (Edit) form.

Procedure 76-29 To view the AA special study statistics data

Perform this procedure to view the AA special study statistics data for subscribers, transit subscribers, SAPs, or spoke SDPs on an ISA-AA MDA. If the ISA-AA group is partitioned, the AA special study tabs appear on the partition.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the required ISA-AA group. The path is Network→NE→Logical Groups→ISA-AA Groups-ISA-AA Group.

3 Right-click on the ISA-AA Group icon and choose Properties from the contextual menu. The ISA-AA Group (Edit) form opens with the General tab displayed.

4 Click on the AA Special Study tab. The following tabs are displayed; each tab lists the corresponding objects in the ISA-AA group:

- Subscribers
- SAPs
- Spoke SDP Bindings
- Transit Subscribers

5 Click on the appropriate tab. A list of objects is displayed.

6 Select an object in the list and click on the Properties button. The AA *object_type* Config (Edit) form opens.

7 Click on the Statistics tab.

8 Choose an AA statistics class from the object drop-down list.

9 Perform one of the following:

a Click on the Collect button to perform an on-demand collection of the current performance statistics data. The collected statistics entries are listed on the form.

b Click on the Collect All button to collect one on-demand statistics record for each statistic type that the object supports. The collected statistics entries are listed on the form.

10 Select an entry in the list and click on the Properties button. The Statistics Record form opens.

11 View the statistics data.

12 Close the Statistics Record form.

13 Close the AA *object_type* Config (Edit) form.

14 Close the ISA-AA Group (Edit) form.

Procedure 76-30 To view AA statistics data for application filters

Perform this procedure to view the application filter hit counts for a local AA group policy.

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Choose AA Group Policy (Application Assurance) from the object drop-down list.

3 Click on the Search button. A list of AA group policies is displayed.

4 Select an AA group policy in the list and click on the Properties button. The AA Group Policy - Global Policy (Edit) form opens with the General tab displayed.

5 Click on the Local Definitions tab.

6 Click on the Search button. A list of local AA group policies is displayed.

7 Select a policy in the list and click on the Properties button. The AA Group Policy - Local Policy (Edit) form opens with the General tab displayed.

8 Click on the Application Filters tab.

9 Click on the Search button. A list of application filters is displayed.

10 Select an application filter in the list and click on the Properties button. The Application Filter - Local Policy (Edit) form opens with the General tab displayed.

11 Click on the Statistics tab.

12 Click on the Collect All button.

13 Click on the Search button. A list of collected statistics is displayed.

14 Select a statistics object in the list and click on the Properties button. The Statistics Record - AA Application Filter Stats form opens.

15 View the statistics data.

16 Close the Statistics Record - AA Application Filter Stats form.

17 Close the Application Filter - Local Policy (Edit) form.

18 Close the AA Group Policy - Local Policy (Edit) form.

19 Close the AA Group Policy - Global Policy (Edit) form.

20 Close the Application Assurance Policies form.

Procedure 76-31 To delete an AA application, application group, or custom protocol

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Choose AA Group Policy (Application Assurance) from the object drop-down list and click on the Search button. A list of AA group policies is displayed.



Note — The 5620 SAM does not create or delete a local AA group policy on each applicable managed NE. A local AA group policy is created or deleted when the ISA-AA group is created or deleted.

3 Select a policy in the list and click on the Properties button. The AA Group Policy (Edit) form opens with the General tab displayed.

4 Perform one of the following.

- **a** Delete an AA application. Click on the Applications tab. A list of AA applications is displayed.
- **b** Delete an application group. Click on the Application Groups tab. A list of application groups is displayed.
- **c** Delete a custom protocol. Click on the Custom Protocols tab. A list of custom protocols is displayed.

5 Select the entry to delete and click on the Delete button. A dialog box appears.

6 Click on the View Dependencies button.



Note — If the application, application group, or custom protocol is associated with a global AA group policy, the dependency count includes all dependencies on the global and local policy instances. When the AA application is on a local AA group policy, the counts include the dependencies on the local policy instance only.

7 Review the dependencies.

8 Click on the OK button.

9 Select the I understand the implications of this action check box.

10 Click on the Yes button. A dialog box appears.

11 Click on the OK button. The object is removed from the list.

12 Click on the Apply button. A dialog box appears.

13 Click on the Yes button.

14 After you delete an AA application, application group, or custom protocol from a global AA group policy, you must distribute the policy changes to each NE that has a local definition of the policy.

To distribute the policy to one or more NEs, perform the following steps.

i Click on the General tab.

ii Click on the Switch Mode button. A dialog box appears.

iii Click on the OK button.

15 Close the AA Group Policy (Edit) form.

Procedure 76-32 To delete an inactive AA transit subscriber instance

Perform this procedure to remove the record of an inactive AA transit subscriber from the 5620 SAM database. An AA transit subscriber instance become inactive when the subscriber is deleted from an AA transit IP policy.



Note 1 — You can use a size constraint policy to ensure that the number of inactive AA transit subscriber instances in the 5620 SAM database remains at a manageable level. See chapter 56 for more information.

Note 2 — AA statistics data can be lost when you delete an AA transit subscriber instance before the 5620 SAM finishes collecting and processing the AA statistics. Alcatel-Lucent recommends that you wait at least two statistics collection intervals before you delete an inactive AA transit subscriber instance.

1 Choose Manage→AA Transit Subscribers from the 5620 SAM main menu. The Manage AA Transit Subscribers form opens.

2 Click on the Search button. A list of AA transit subscriber instances is displayed.

3 Click on the Active column header to sort the list. An inactive AA transit subscriber instance has no check mark in the Active column.

4 Select the AA transit subscriber instance to delete and click on the Delete button. The AA transit subscriber instance is removed from the list.

5 Close the Manage AA Transit Subscribers form.

77 — Service Test Manager

77.1 Service Test Manager overview *77-2*

77.2 Sample Service Test Manager implementation *77-4*

77.3 Sample network monitoring configuration *77-7*

77.4 Sample network monitoring configuration steps *77-8*

77.5 Sample SAA accounting files configuration *77-14*

77.6 Sample SAA accounting files configuration steps *77-14*

77.7 Sample threshold-crossing alarm configuration *77-16*

77.8 Sample threshold-crossing alarm configuration steps *77-17*

77.9 7210 SAS Y.1564 service test *77-19*

77.10 Sample 7210 SAS Y.1564 service test configuration steps *77-20*

77.11 Sample OmniSwitch device SLA testing *77-26*

77.12 Workflow to use the Service Test Manager *77-31*

77.13 Service Test Manager procedures *77-33*

77.1 Service Test Manager overview

The 5620 SAM service test manager (STM) provides the ability to group various OAM tests into test suites for network troubleshooting and for verifying compliance with SLAs. You can schedule the execution of a test suite to provide continual performance feedback, or run a test suite on demand to investigate service issues. The test results are logged for monitoring and trend analysis.

The grouping of tests into a test suite allows a 5620 SAM operator to use one schedule for the periodic execution of multiple OAM diagnostics against multiple network objects; for example, services, NEs, or transport components. An operator can choose to include existing tests, use the 5620 SAM to generate the tests that comprise a test suite, or both. Groups of tests in a suite can be configured to execute sequentially or concurrently. In addition, you can configure a test suite as an OAM validator to verify the operational status of a service. This can also be done on a one-time basis using the One Time Validation function.

You can configure threshold-crossing parameters to generate alarms when rising or falling threshold values are reached due to the reach, latency, or jitter issues discovered by the OAM tests.

The 5620 SAM STM allows the deployment of the maximum number of tests to a 7450 ESS, 7750 SR, or 7950 XRS. The 5620 SAM raises an alarm when the number of tests on an NE is 60% of the configured maximum. Attempts to create or execute a test using the 5620 SAM fail when the number of deployed tests on an NE is too high.

Test policies

To enable the automatic generation of tests for a test suite, the 5620 SAM requires a test policy that contains a set of test definitions and pre- and post-processing rules. A test policy also specifies the order of execution for the generated tests. A test policy applies to only one test suite, and a test suite can have only one associated test policy.

Test policy parameters can be configured to only display test results if a test fails or generates a threshold crossing alarm. In large networks, this can substantially reduce the amount of test data that the 5620 SAM needs to collect.

A test policy is specific to one type of entity; for example, a VLL service or service tunnel. The test definitions in the policy are restricted to the tests that apply to the entity type specified in the policy. A test policy is applied to a test suite during test suite creation.

Test suites

A test suite contains three test groups:

- **First-run tests**
  First-run tests are the tests in a suite that the 5620 SAM executes before the tests in the other groups. First-run tests are chosen from a list of existing tests and might typically include high-level diagnostics; for example, a service site ping or VPRN ping. No restrictions apply to the types of tests that are selectable as first-run tests.

- **Generated tests**

  Generated tests are created by the 5620 SAM for use against a specific network entity, based on the entity type specified in the suite and the specific tested entities that are named in the associated test policy. For example, a service site ping test policy associated with a three-site VPRN test suite causes the 5620 SAM to generate six tests: one site ping test from each site in the VPRN to the other two sites. When you change the configuration of a network entity, such as a service, you must regenerate the generated tests that apply to the entity. Test regeneration removes previously generated tests from a test suite.
- **Last-run tests**

  Last-run tests are the tests in a suite that the 5620 SAM executes after the tests in the other groups. Last-run tests are chosen from a list of existing tests and might typically include transport-layer diagnostics; for example, an LSP trace or a tunnel ping. No restrictions apply to the types of tests that are selectable as last-run tests.

To create a test suite that contains tests for different entity types, you can specify that the test suite applies to no specific entity type. In this way, you can create a group of disparate tests to which no test policy restrictions apply. Specifying none as the entity type in a test suite has the following effects.

- It allows you to choose any predefined test as a first-run or last-run test.
- It disables test generation in the test suite, because test generation requires a test policy that is based on a specific entity type.



Note 1 — The 5620 SAM does not attempt to discover tests or test suites that are configured locally on an NE, for example, using a CLI.

Note 2 — If you attempt to modify an OAM test or test suite that is deployed to a suspended NE, the 5620 SAM raises an alarm.

To manage the system resources that test execution consumes, the 5620 SAM assigns a weight value to a test. When the 5620 SAM executes a test, it attempts to reserve the test weight from a resource pool, performs the test, then returns the test weight to the pool. The weight of a test suite is the sum of the weights of the individual tests in the suite. The 5620 SAM attempts to reserve the weight of the whole suite for the duration of suite execution. If the required weight for a test or test suite is unavailable, execution is halted and the Status value contained in the test result is set to Not Enough Resources.

You can create an OAM service validation test to verify the operational status of a service. The operational status of a service depends on the operational states of its service sites or instances. It is possible for a service to be operationally up when communication between sites is not operational. For example, a VRF can be operationally up but the routes to its peers might not be populated because of the routing policy, route target, or ACL configuration. The State Cause of the service indicates the success or failure of the OAM validation test, and therefore, service connectivity.

You can configure an OAM validator when you create a test suite and run the OAM validation test from the service configuration form.

Note — OAM validation tests are not supported for HVPLS.

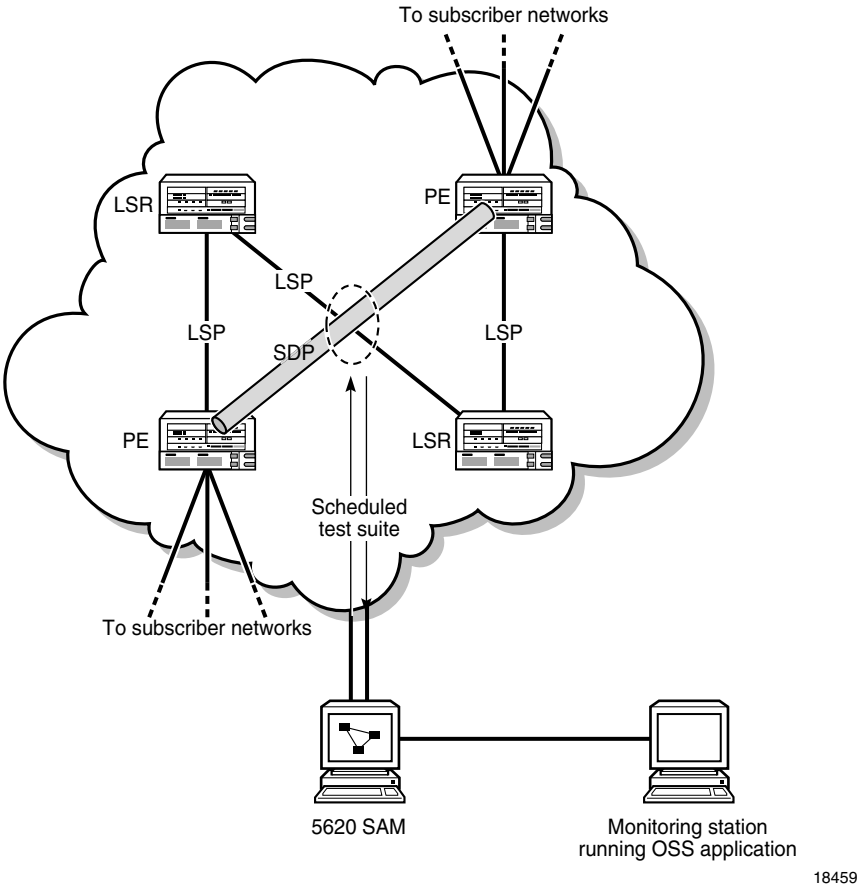
Consider the following when you create or execute test suites.

- A test, whether pre-existing or generated, is associated with only one test suite.
- You can execute a generated test on demand, not just in the context of a test suite.
- STM test suites can be configured as scheduled tasks. See chapter 7 for information about using the 5620 SAM to schedule tasks.
- Using an NE schedule does not ensure that the target NEs perform the actions in an associated STM scheduled task in the order specified; the NEs that execute an NE scheduled task operate independently and are not directed by the 5620 SAM. As soon as an NE completes an action in an NE scheduled task, it performs the next action.
- The 5620 SAM database logs test results only for scheduled test suites that are associated with SAM schedules. Logging for test suites that are associated with NE schedules is performed locally on each target NE.
- Size constraint policies control the number of historical records that the 5620 SAM retains in the database. You can configure size constraint policies to limit the number of database objects that are associated with specific test types. See chapter 42 for information about size constraint policies.
- A 5620 SAM user who is assigned the admin or QoS/ACL management scope of command role can create and modify all tests, test policies, and test suites. A user who is assigned the service management scope of command role can create and modify only STM components that are related to services. A user who is assigned the topology management role can create and modify only STM components that are related to network transport elements.
- OAM test suites in which the Validation Test Suite parameter is enabled are used to test the operational status of a service or service-related entity such as a service tunnel. The result of this validator test is indicated by the OAM Validation Failed state cause indicator on the General tab of the management form for the object.
- You can view test suite results for an object from the Tests tab of the configuration form for the object.

77.2 Sample Service Test Manager implementation

Figure 77-1 shows a sample STM implementation that illustrates how you can use STM suites to verify service operation and identify network problems.

Figure 77-1 Sample STM implementation



In the sample network, two scheduled STM test suites run constantly to ensure that the transport elements are functioning properly. One test suite monitors the SDPs, and the other test suite monitors the LSPs. A 5620 SAM administrator can quickly update the test suites, as required, to reflect network topology changes by revising the list of tested entities in the suite and regenerating the tests. An OSS application collects the test result information which is then available for monitoring by NOC staff.

Note — This sample configuration uses a SAM schedule to create a scheduled task. See chapter 7 for information about SAM schedules.

The SDP test suite contains the following generated tests for each SDP:

- tunnel ping
- MTU ping

The LSP test suite contains the following generated test for each LSP path:

- LSP ping (tested entity type is LSP path)

NOC monitoring staff become aware that tunnel ping operations fail occasionally on one SDP. Packet loss is not yet significant enough to affect SLAs, but threatens to become so, based on the observed trend. NOC staff run a test suite against the LSPs in the affected LSP path. The test suite contains the following generated test for each LSP in the LSP path:

- LSP ping (tested entity type is LSP)

Test results show that the packet loss is related to a specific LSP in the path. Investigation of the LSP traffic pattern indicates that a recently provisioned service is causing the LSP to be oversubscribed. The problem is addressed by a network designer and is corrected through configuration changes.

Table 77-1 lists the high-level tasks necessary to configure and use the STM elements in this sample.

Table 77-1 Sample STM implementation configuration sequence

Task	Description
1. Scheduled STM test-suite creation	Create STM test policies for transport-layer elements. • Create a test policy for the SDPs. Specify Tunnel (SDP) as the Entity Type for the policy, and choose Tunnel Ping and MTU Ping as the test definitions. Create separate tunnel ping definitions for different forwarding classes, as required. • Create a test policy for the LSP paths. Specify LSP as the Entity Type for the policy and choose LSP Ping as the test definition. In the test definition, specify LSP Path as the Target Type. Create separate LSP ping definitions for different forwarding classes, as required. Create STM test suites for transport-layer elements. • Create a test suite for the SDPs. Specify Tunnel (SDP) as the Entity Type for the suite, choose the SDP test policy, choose the SDPs against which the suite is to run, and use the 5620 SAM to generate the tests in the suite. Create a schedule for the test suite according to network monitoring requirements, and apply the schedule to the test suite to create a scheduled task. • Create a test suite for the LSP paths. Specify LSP as the Entity Type for the suite, choose the LSP test policy, choose the LSP paths against which the suite is to run, and use the 5620 SAM to generate the tests in the suite. Create a schedule for the test suite according to network monitoring requirements, and apply the schedule to the test suite to create a scheduled task.
2. Data presentation	Customize the tabular display of test results in the 5620 SAM, or create an OSS application that retrieves test-result data from the 5620 SAM and presents it as information in graphical format for NOC staff.
3. Creation of non-scheduled STM test suite or individual OAM tests for network troubleshooting	Create an STM test policy for the LSPs for use during network troubleshooting. • Create a test policy for the LSPs. Specify LSP as the Entity Type for the policy and choose LSP Ping as the test definition. In the test definition, specify LSP as the Target Type. Create separate LSP ping definitions for different forwarding classes, as required. Create a non-scheduled STM test suite (or individual OAM tests, depending on the number of LSPs involved) for the LSPs in the LSP path. • Specify LSP as the Entity Type for the suite, choose the newly created LSP test policy, choose the LSPs in the LSP path against which the suite is to run, and use the 5620 SAM to generate the tests for the suite.
4. Network monitoring	Use the 5620 SAM to display the scheduled test results in tabular format, or use an OSS application to monitor the LSP ping, tunnel ping, and MTU ping diagnostic results in real time. Record inconsistencies and trends, and troubleshoot the network as required. Use the threshold-crossing alarm capabilities to raise alarms when traffic characteristics rise above or fall below specific values.

(1 of 2)

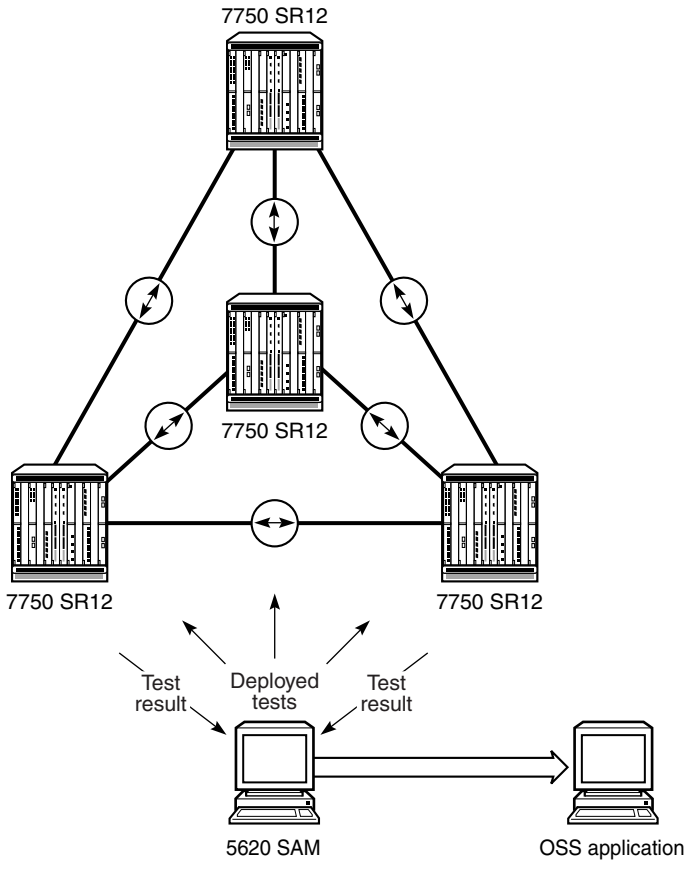
Task	Description
5. Network troubleshooting	When potential trouble arises, use a non-scheduled STM test suite or individual STM tests to help identify the cause. • Create individual tests or edit the existing non-scheduled test suite. Include as tested entities the LSPs that comprise the LSP path and regenerate the tests for the suite, as required. • Execute the non-scheduled test suite and monitor the test results. • Edit the test definition in the test policy. Change test parameter values as required, regenerate the tests in the suite, and re-execute the suite. Continue to refine the diagnostic test results until the problem manifests itself in the test results.

(2 of 2)

77.3 Sample network monitoring configuration

Figure 77-2 shows the high-level flow of tests and test results in a simple network topology that the network provider wants to continually monitor using the STM. See section 77.4 for the explicit steps required to create the STM configuration.

Figure 77-2 Continual network topology monitoring



A 5620 SAM administrator creates and schedules an STM test suite to monitor the LSP mesh and identify potential overloading and reachability problems before they affect service traffic. The test suite contains ping and trace test definitions for three different classes of in-profile traffic and is scheduled to run every 15 minutes.



Note — This sample configuration uses a SAM schedule to create a scheduled task. See chapter 7 for information about SAM schedules.

Because the same group of tests is to be run on multiple entities of the same type, the test suite consists of generated tests only. The test policy that the 5620 SAM uses to generate the tests contains the following six test definitions:

- LSP ping - be in
- LSP ping - af in
- LSP ping - nc in
- LSP trace - be in
- LSP trace - af in
- LSP trace - nc in

The 5620 SAM generates 72 tests for the test suite—3 ping tests and 3 trace tests for each of the 12 LSPs and LSP paths. Every 15 minutes, the 5620 SAM scheduler executes the tests and stores the results. An OSS application periodically retrieves the test results, performs trend analysis and presents the transport utilization information to NOC monitoring staff.

The 5620 SAM generates an alarm in the event of an LSP ping probe failure or an LSP trace path change, as specified in the test policy, so 5620 SAM operators become aware of new transport faults as they arise.

77.4 Sample network monitoring configuration steps

The following steps explicitly define the end-to-end configuration of the network monitoring sample in section 77.3. For conciseness, the procedure lists only the configuration steps and parameters that are specific to and necessary for the sample. See the procedures in section 77.13 for complete STM configuration information.

Create test policy for test generation

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Create Test Policy from the Create contextual menu. The Test Policy (Create) form opens.

4 Configure the parameters in Table 77-2 using the supplied values:

Table 77-2 Test policy General tab parameters

Parameter	Value	Comment
Name	LSP Test Policy	—
NE Schedulable	disabled	NE-schedulable test results are not returned to the 5620 SAM.
Entity Type	LSP	—

5 Click on the Test Definitions tab.

6 Click on the Add button to add a test definition to the test policy. A menu appears.

7 Choose MPLS→Add LSP Ping. The LSP Ping Definition (Create) form opens with the General tab displayed.

In the sample configuration, the operator creates a separate LSP Ping test definition for each of the following forwarding classes:

- be (best effort - low priority, delivery not guaranteed)
- af (assured forwarding - medium priority, delivery guaranteed)
- nc (network control - high priority, delivery guaranteed)

8 Configure the parameters in Table 77-3 using the supplied values, most of which are common to the three test definitions:

Table 77-3 LSP Ping Definition parameters

Parameter	Value	Comment
General tab		
Name	LSP Ping - be in LSP Ping - af in LSP Ping - nc in	First test definition Second test definition Third test definition
Target Type	LSP	—
Test parameters tab		
Number of Test Packets	5	This provides more analysis granularity than a single test packet without affecting network performance.
Size (octets)	108	This is the minimum packet size for this type of test on the 7450 ESS and 7750 SR. The minimum packet size varies, depending on the type and release of device against which a test runs.
Forwarding Class	be af nc	For LSP Ping - be in test definition For LSP Ping - af in test definition For LSP Ping - nc in test definition To cover a range of traffic streams and to test different network queues, multiple test definitions are necessary. The sample configuration uses three LSP ping definitions that differ only by forwarding class.
Forwarding Profile	in	All test packets are marked in-profile. This means that they follow the same path as service traffic.

(1 of 2)

Parameter	Value	Comment
Results configuration tab		
Probe History Size (rows)	100	—
Trap Generation	Probe Failure	Test-probe failures provide early notification of LSP congestion or reachability issues to a 5620 SAM operator. OSS analysis of the results indicates trends for further investigation.

(2 of 2)

9 Click on the OK button. The LSP Test Definition (Create) form closes and a dialog box appears.

10 Click on the OK button. The test definition is listed on the Test Policy (Create) form.

11 Repeat steps 6 to 10 for the remaining test definitions listed in step 7.

12 Click on the Add button to add a test definition to the test policy. A menu appears.

13 Choose MPLS→Add LSP Trace. The LSP Trace Definition (Create) form opens with the General tab displayed.

In the sample configuration, the operator creates a separate LSP Trace test definition for each of the following forwarding classes:

- be (best effort - low priority, delivery not guaranteed)
- af (assured forwarding - medium priority, delivery guaranteed)
- nc (network control - high priority, delivery guaranteed)

14 Configure the parameters in Table 77-4 using the supplied values. Values that are not common to the three test definitions are so indicated.

Table 77-4 LSP Trace Definition parameters

Parameter	Value	Comment
General tab		
Name	LSP Trace - be in LSP Trace - af in LSP Trace - nc in	For first test definition For second test definition For third test definition
Target Type	LSP Path	—
Test parameters tab		
Number of Test Packets	5	This provides more analysis granularity than a single test packet without affecting network performance.
Size (octets)	108	This is the minimum packet size for this type of test on the 7450 ESS and 7750 SR. The minimum packet size varies, depending on the type and release of device against which a test runs.

(1 of 2)

Parameter	Value	Comment
Forwarding Class	be af nc	For LSP Trace - be in definition For LSP Trace - af in definition For LSP Trace - nc in definition To cover a range of traffic streams and to test different network queues, multiple test definitions are necessary. The sample configuration uses a different LSP ping definition for each forwarding class.
Forwarding Profile	in	All LSP ping test definitions in the sample involve in-profile traffic.
Results configuration tab		
Probe History Size (rows)	100	—
Trap Generation	Test Failure Path Change	A test failure trap may indicate a routing or congestion issue, but it also indicates test misconfiguration when the Maximum Time to Live parameter value is too low to allow a test probe to reach the destination LSP. A path change trap may indicate an intermittently congested or unresponsive LSP.

(2 of 2)

15 Click on the OK button. The LSP Test Definition (Create) form closes and a dialog box appears.

16 Click on the OK button. The test definition is listed on the Test Policy (Create) form.

17 Repeat steps 12 to 16 for the remaining test definitions listed in step 13.

18 Click on the OK button. A dialog box appears.

19 Click on the Yes button. The Test Policy (Create) form closes and the Service Test Manager form reappears.

Create schedule

20 Choose Tools→Schedules→Schedule from the 5620 SAM main menu. The Schedule form opens.

21 Click on the Create button and choose Create SAM Schedule. The SAM Schedule (Create) form opens.

22 Configure the parameters in Table 77-5 using the supplied values:

Table 77-5 SAM Schedule parameters

Parameter	Value	Comment
Name	LSP Assurance	—

(1 of 2)

Parameter	Value	Comment
Current Client Start Time	a future time	Specify the date and time at which the schedule is to be first triggered. This value is used to calculate the times of subsequent triggers, based on the Frequency parameter value. Compare this value and the Frequency parameter value with those in other 5620 SAM schedules to ensure that the schedule trigger times are staggered and the resulting NE task load is balanced.
Ongoing	enabled	This setting tells the 5620 SAM to continually trigger execution of the task associated with the schedule.
Frequency	Per Minute / 15	You must also select the Run Every Minutes radio button and specify 15 as the number of minutes for the triggering frequency.

(2 of 2)

23 Click on the OK button. The SAM Schedule (Create) form closes.

24 Close the Schedule form.

Create test suite

25 Click on the Create button in the Service Test Manager form and choose Create Test Suite from the contextual menu. The Test Suite (Create) form opens with the General tab displayed.

26 Configure the parameters in Table 77-6 using the supplied values.

Table 77-6 Test suite parameters

Parameter	Value	Comment
Name	LSP Test Suite	—
Entity Type	LSP	—
NE Schedulable	disabled	NE-schedulable test results are not returned to the 5620 SAM.

27 Click on the Test Policy tab.

28 Click on the Add button to choose a test policy that governs the generation of tests in the test suite. The Select Test Policy - Test Suite form opens.

29 Configure the filter properties and click on the Search button. A list of test policies is displayed.

30 Select the LSP Test Policy entry and click on the OK button. The test policy is listed on the Test Suite (Create) form.

31 Click on the Tested Entities tab.

32 Click on the Add button to choose the LSPs that are to be regularly assessed by the test suite. The Select Tested Entity - Test Suite form opens.

33 Configure the filter properties and click on the Search button to display a list of LSPs.

34 Select the LSPs that you want to include and click on the OK button. The LSPs are listed on the Test Suite (Create) form.

35 Click on the Apply button to save the changes. Additional buttons appear and the form name changes to Test Suite (Edit).

36 Click on the Generated Tests tab.

37 Click on the Generate Tests button. The 5620 SAM generates a test for each LSP listed on the Tested Entities tab. The tests are listed on the form as they are generated.

Apply a span of control to a test suite

38 Click on the Spans tab.

39 Click on the Add button. The Select Spans - Test Suite form opens with a list of available spans.

40 Select one or more spans to apply to the test suite.

41 Click on the OK button. The Select Spans - Test Suite form closes and a dialog box appears.

42 Click on the OK button to confirm the action.

Create scheduled task

43 Click on the Schedule button and choose Create SAM Scheduled Task. The SAM Scheduled Task (Create) form opens with LSP Test Suite displayed in the Task panel.

44 Configure the parameters in Table 77-7 using the supplied values.

Table 77-7 SAM scheduled task parameters

Parameter	Value	Comment
Scheduled Task Name	Periodic LSP Check	—
Administrative State	Enabled	The 5620 SAM executes the scheduled task at regular intervals based on the specified Current Client Start Time and Frequency.

45 Click on the Select button. The Select Schedule - SAM Scheduled Task form opens.

46 Select LSP Assurance and click on the OK button. The 5620 SAM automatically populates the Schedule panel with the schedule information.

47 Click on the OK button. The SAM Scheduled Task (Create) form closes and the Test Suite (Edit) form reappears.

48 Close the Test Suite (Edit) form.

49 Close the Service Test Manager form.

77.5 Sample SAA accounting files configuration

The following sample configuration focuses on the configuration of SAA accounting files that are to be collected following the generation of an NE schedulable test of VLL services.

A network provider wants to use the 5620 SAM to view test result information for a NE schedulable test of VLL services and wants the 5620 SAM to process the OAM results MIB entries and produce a compressed XML record that is stored in SAA accounting files on the nodes.

A 5620 SAM administrator must create an NE schedulable test for VLL services that records test result information in SAA accounting files. The administrator creates one accounting policy, one file policy, one test policy, and one test suite. Section 77.6 describes the steps that are required to create a test.

77.6 Sample SAA accounting files configuration steps

The following steps explicitly define the end-to-end configuration of the SAA accounting files sample in section 77.5. For conciseness, the procedure lists only the configuration steps and parameters that are specific to and necessary for the sample. See the procedures in section 77.13 for complete STM configuration information.

Create accounting policy

1 Choose Tools→Statistics→Accounting Policies from the 5620 SAM main menu. The Manage Accounting Policies form opens.

2 Click on the Create button. The Accounting Policy (Create) form opens.

3 Configure the parameters in Table 77-8 using the supplied values.

Table 77-8 Accounting policy parameters

Parameter	Value	Comment
Displayed Name	SAA Accounting Policy	—
Type	NE Schedulable Tests	You must choose this value to allow the configuration of SAA accounting files

4 Click on the Select button beside the File ID parameter. The Select A File Policy form opens.

5 Click on the Create button. The File Policy (Create) form opens.

6 Configure the Displayed Name parameter. For the purposes of this sample, the value shall be SAA File Policy.

7 Click on the OK button. The File Policy (Create) form closes and the Select A File Policy form reappears.

8 Select the SAA File Policy entry and click on the OK button. The Select A File form closes and the file policy is listed on the Accounting Policy (Create) form.

9 Click on the OK button. The Accounting Policy (Create) form closes and the Manage Accounting Policies form reappears.

10 Configure the filter properties and click on the Search button. A list of accounting policies is displayed

11 Select the SAA Accounting Policy entry and click on the Distribute button. The Distribute form opens.

12 Select the entities that you want to include and click on the OK button. The Distribute form closes.

13 Close the Manage Accounting Policies form.

Create test policy

14 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

15 Click on the Create button.

16 Choose Create Test Policy from the Create contextual menu. The Test Policy (Create) form opens.

17 Configure the parameters in Table 77-9 using the supplied values:

Table 77-9 Test policy parameters

Parameter	Value	Comment
Name	SAA Test Policy	—
NE Schedulable	enabled	You must enable this parameter to allow the configuration of SAA accounting files.
Entity Type	VLL Service	—
Accounting Files	enabled	You must enable this parameter to allow the configuration of SAA accounting files.

18 Click on the Test Definitions tab.

19 Click on the Add button to add a test definition to the test policy. A menu appears.

20 Choose Service→Add VCCV Ping. The VCCV Ping Definition (Create) form opens with the General tab displayed.

21 Click on the OK button. The VCCV Ping Definition (Create) form closes and a dialog box appears.

22 Click on the OK button. The test definition is listed on the Test Policy (Create) form.

23 Click on the OK button. The Test Policy (Create) form closes and the Service Test Manager form reappears.

Create test suite

24 Click on the Create button in the Service Test Manager form and choose Create Test Suite from the contextual menu. The Test Suite (Create) form opens with the General tab displayed.

25 Configure the parameters in Table 77-10 using the supplied values:

Table 77-10 Test suite parameters

Parameter	Value	Comment
Name	SAA Test Suite	—
Entity Type	VLL Service	—
NE Schedulable	enabled	You must enable this parameter to allow the configuration of SAA accounting files.

26 Click on the Test Policy tab.

27 Click on the Add button to choose a test policy that governs the generation of tests in the test suite. The Select Test Policy - Test Suite form opens.

28 Configure the filter properties and click on the Search button. A list of test policies is displayed.

29 Select the SAA Test Policy entry and click on the OK button. The test policy is listed on the Test Suite (Create) form.

30 Click on the Tested Entities tab.

31 Click on the Add button. The Select Tested Entity - Test Suite form opens.

32 Configure the filter properties and click on the Search button to display a list of entities.

33 Select the nodes that were used in step 12 and click on the OK button. The nodes are listed on the Test Suite (Create) form.

34 Click on the Apply button to save the changes. Additional buttons appear and the form name changes to Test Suite (Edit).

35 Click on the Generated Tests tab.

36 Click on the Generate Tests button. The 5620 SAM generates a test for each entity listed on the Tested Entities tab. The tests are listed on the form as they are generated.

77.7 Sample threshold-crossing alarm configuration

The following sample configuration focuses on the configuration of a threshold-crossing alarm that is to be included in a test suite. It does not describe the configuration of the test suite, schedule or scheduled task associated with the sample. No test policy is required for the configuration, as it does not involve generated tests.

A network provider wants to use the 5620 SAM to monitor a customer VPLS named VPLS 17 that carries VoIP traffic. He wants the 5620 SAM to raise an alarm when the round-trip jitter value rises above a specified threshold.

Network jitter values typically range from 10 to 15 ms, but are occasionally as high as 25 ms. Jitter buffers in the end-user VoIP sets can accommodate up to 80 ms of jitter. A network engineer determines that a jitter test threshold of 30 ms is low enough to allow NOC operators sufficient time for investigating a jitter increase, yet high enough to exclude spurious jitter events.

A 5620 SAM administrator wants to creates a scheduled CPE ping test suite for the VPLS that periodically measures the round-trip jitter between each VPLS site and an end device. The administrator creates one CPE ping test for each site in the VPLS. Section 77.8 describes the steps required to create one such test.

77.8 Sample threshold-crossing alarm configuration steps

The following procedure explicitly defines the configuration steps required to create the test with a threshold-crossing alarm described in section 77.7. See section 77.4 for information about sample test-suite, test policy, or scheduling configurations. See the procedures in section 77.13 for complete STM configuration information.

For conciseness, the procedure lists only the configuration steps and parameters that are specific to and necessary for the sample.

Create CPE ping test with threshold-crossing criteria

1 Click on the Create button in the Service Test Manager form and choose L2 Service→CPE ping from the contextual menu. The CPE Ping Test (Create) form opens with the General tab displayed.

2 Configure the parameters in Table 77-11 using the supplied values:

Table 77-11 General CPE Ping test parameters

Parameter	Value	Comment
General tab		
Name	CPE Ping Test - VPLS 17, Site A	A descriptive name such as this is helpful for quickly identifying the entity under test when viewing the test results.
NE Schedulable	enabled	You must enable this parameter to allow the configuration of threshold-crossing criteria.
Select button in Service panel	VPLS 17	Click on the Search button on the Select Service - CPE Ping form that opens to choose a service.
Select button in Site panel	Site A	Click on the Search button on the Select Site - CPE Ping form that opens to choose a service.
Destination Path Address	*IP address of an end device connected to Site A*	This is the IP address to which the CPE ping packets are sent.
Source IP Address	*IP address of the NE that originates the test packets*	This IP address must be in the same subnet as the Destination IP Address.

(1 of 2)

Parameter	Value	Comment
Source MAC Address	*MAC address of the NE that originates the test packets*	—
Test parameters tab		
Number of Test Packets	5	This provides more analysis granularity than a single test packet without affecting network performance.
Results configuration tab		
Probe History Size (rows)	100	This value provides a greater retained test-result history for occasional monitoring by a 5620 SAM operator.
Trap Generation	Probe Failure	Test-probe failures provide early notification of congestion or reachability issues to a 5620 SAM operator for troubleshooting purposes.

(2 of 2)

3 Click on the Apply button. Additional buttons and tabs appear, and the form name changes to CPE Ping *Test Name* (Edit).

4 Click on the Threshold Alarms tab.

5 Click on the Add button to add threshold criteria. The NE Threshold Event (Create) form opens with the General tab displayed.

6 Configure the parameters in Table 77-12 using the supplied values:

Table 77-12 Threshold-crossing CPE Ping test parameters

Parameter	Value	Comment
Type	Round-Trip Jitter	—
Generate Alarm on Rising Threshold	enabled	This is the default setting. Alternatively or additionally, by enabling the Generate Alarm on Rising Threshold parameter, you can configure the 5620 SAM to generate an alarm when a test-result value falls below a specified threshold. You can also configure the 5620 SAM to clear a rising-threshold alarm when the test-result value falls below the value configured for the falling threshold.
Rising Threshold tab		
Threshold Value	30	This value specifies that the 5620 SAM is to generate an alarm when an individual test result contains a round-trip jitter value greater than 30 ms.

7 Click on the OK button. The NE Threshold Event (Create) form closes.

8 Close the CPE Ping *Test Name* (Edit) form.

77.9 7210 SAS Y.1564 service test

The 5620 SAM supports ITU-T Y.1564 tests for Ethernet service configuration and performance. Y.1564 provides a standard for measuring throughput, latency, frame loss, and jitter to assess whether the tested service complies with an SLA.

The following 7210 SAS devices support Y.1564 service tests:

- 7210 SAS-D, Release 6.0 R2 or later
- 7210 SAS-M (in access-uplink mode), Release 5.0 R4 or later
- 7210 SAS-M (in network mode), Release 6.0 R2 or later

You can configure a supported 7210 SAS NE as a test-head for performing Y.1564 bidirectional throughput tests on an Epipe service. The test-head generates test data up to the configured line rate and sends it through the service from the source SAP to the remote SAP. The remote SAP performs a port loopback with MAC swap and returns the test data to the source SAP. The test-head analyses the data and produces the test results. You can assign a no-service access port as the test-head port on the 7210 SAS test-head NE. The source SAP for the service you are testing must reside on the same NE.

A test-head profile specifies the parameters for the test, including duration, line rate, frame payload, and acceptance criteria. Profiles are created and distributed using the 5620 SAM policy framework. See chapter 42 for more information.

You can create, save, and execute Y.1564 bidirectional tests for a configured Epipe service using the 5620 SAM Service Test Manager. Alternatively, you can use the Tests tab of the properties form for the service. To prevent service disruptions when other services share the ports on which the source SAP and remote SAP are configured, the 5620 SAM provides a function to move the SAPs to target ports where no services are configured. See Chapter 81 for more information.

You can add the Y.1564 bidirectional test to a 5620 SAM test suite as a first-run or last-run test, and you can use the test suite to schedule the test. Consider the following when you add the Y.1564 bidirectional test to a test suite:

- Test policies are not supported
- Generated tests are not supported
- The Y.1564 bidirectional test is not NE-schedulable
- Parallel tests are not supported. You can run only one Y.1564 bidirectional test at a time.

The system resource profile for the 7210 SAS test-head NE must be configured appropriately. You must allocate a minimum of four entries to the ingress internal ACL MAC resource pool, and a minimum of two entries to the egress internal resource pool (ACL MAC, IPv4 or IPv6 64-bit criteria). The test-head tool uses resources from these resource pools. If no resources are available in these pools, the test-head tool cannot function. You must not allocate resources to the egress internal ACL 128-bit IPv6 criteria. See "System resource profile" in section 8.5 and Procedure 13-20 for more information about configuring the system resource profile.

See the *7210 SAS M, X OS OAM and Diagnostic Guide* for more information about the Y.1564 test-head function.

Workflow to configure and execute Y.1564 bidirectional tests

See section 77.10 for sample 7210 SAS Y.1564 service test configuration steps. The service to be tested must already be configured in the 5620 SAM.

1 Ensure that the system resource profile for the 7210 SAS test-head NE is configured appropriately. See Procedure 13-20.

2 Ensure that the OLC state of the service to be tested is set to maintenance. See Procedure 67-1.

3 Select a test-head port on the applicable 7210 SAS NE. The source SAP for the service to be tested must be on the same NE.

4 Create a test-head profile and distribute the profile to the 7210 SAS NE that contains the test-head port and the source SAP of the service to be tested.

5 Configure the Y.1564 bidirectional test in the 5620 SAM Service Test Manager.

6 Move SAPs as required. See Chapter 81 for more information.

7 Add the Y.1564 bidirectional test to a test suite, if required. See Procedure 77-4 and the overview to this section, above.

8 Execute the test and view the results.

9 Restore the original SAP configuration, if required.

77.10 Sample 7210 SAS Y.1564 service test configuration steps

The following procedures list only the configuration steps and parameters that are required for the sample. See the procedures in section 77.13 for complete STM configuration information.

Select a test-head port



Note — You must configure the test-head port on the 7210 SAS NE that contains the source SAP of the service you need to test.

You can configure a test-head port on the following 7210 SAS devices:

- 7210 SAS-D, Release 6.0 R2 or later
- 7210 SAS-M (in access-uplink mode), Release 5.0 R4 or later
- 7210 SAS-M (in network mode), Release 6.0 R2 or later

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the 7210 SAS NE on which you need to configure a test-head port and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Globals tab.

4 Click on the Service tab.

5 Click on the Select button in the TestHead Port section of the Loopback No Service Ports panel. A list of access ports appears.

6 Choose a port in the list and click on the OK button. The NE properties form reappears with the TestHead Port name displayed.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The NE properties form closes.

Create a test-head profile



Note — The test-head profile is distributed to the NE using the 5620 SAM policy distribution framework. See Chapter 42. You must distribute the test-head profile for the Y.1564 bidirectional test to the source site for the service that you are testing.

9 Choose Tools → Y1564 Test Head Profile from the 5620 SAM main menu. The Y1564 Test-Head Profiles form opens.

10 Click on the Create button. The Y1564 Test-Head Profile, Global Policy (Create) form opens with the General tab displayed.

11 Configure the parameters:

- Auto Assign ID
- Profile ID
- Description
- Frame Size
- Enable Test Completion Trap
- Hours (Hr)
- Minutes (Min)
- Seconds (Sec)
- CIR (Admin)(kbps)
- Adaptation Rule

12 Click on the Frame Payload tab.

13 Click on the Create button. The Y1564 Test-Head Payload, Y1564 Test-Head Profile, Global Policy (Create) form opens.



Note — You can create up to four Frame Payload configurations for each test-head profile.

14 Configure the parameters:

- ID
- Description
- Type
- Ether Type
- Source MAC Address
- Destination MAC Address
- Data Pattern
- VLAN Tag 1
- VLAN Tag 2
- IP Protocol
- IP Type of Service
- DSCP
- Time To Live
- Source IP Address
- Source Port
- Destination IP Address
- Destination Port

The parameters that are configurable depend on the option you choose for the Type parameter.

15 If you configured a value for the VLAN Tag 1 parameter, configure the parameters in the VLAN Tag 1 panel:

- TpID
- Dot1pID

Otherwise, go to step 17.

16 If you configured a value for the VLAN Tag 2 parameter, configure the parameters in the VLAN Tag 2 panel:

- TpID
- Dot1pID

17 Click on the OK button. A dialog box appears.

18 Click on the OK button.

19 Click on the Acceptance Criteria tab.

20 Click on the Create button. The Y1564 Test Head Acceptance Criteria, Y1564 Test Head Profile, Global Policy (Create) form opens.



Note — You can create up to four Acceptance Criteria configurations for each test-head profile.

21 Configure the parameters:

- Acceptance Criteria ID
- Default
- Jitter Threshold (microseconds)
- Default
- Latency Threshold (microseconds)
- Default
- Loss Threshold

22 Click on the OK button. A dialog box appears.

23 Click on the OK button. The Y1564 Test-Head Profile, Global Policy (Create) form reappears.

24 Click on the Apply button. The Y1564 Test-Head Profile, Global Policy (Create) form reappears with additional buttons.

25 Click on the General tab. The form is displayed with the Policy Configuration panel added.

26 Click on the Switch Mode button to change the Configuration Mode to Released. A dialog box appears.

27 Click on the Yes button. The Release - Y1564 Test-Head Profile form opens.

28 Select the required NEs and click on the Distribute button to manually distribute the policy to the NEs. You must distribute the test-head profile to the source site for the VLL Epipe service to be tested. The source site must be a 7210 SAS that supports Y.1564 bidirectional tests.

Configure and execute the test using the 5620 SAM Service Test Manager



Note — You can only configure tests for VLL Epipe services that are fully configured in the 5620 SAM.

29 Configure initial test settings.

i Choose Tools→ Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager (STM) form opens. Alternatively, you can configure tests from the Tests tab of the properties form for the service you need to test.

ii Click on the Create button and choose Service → Y1564 BiDirectional Test from the contextual menu. The Y1564 Bi-Directional Test (Create) form opens, with the General tab displayed.

iii Configure the parameters:

- Auto-Assign ID
- ID
- Name
- Description
- Administrative State

30 Choose a service for the test.

i In the Service panel, click on the Select button. The Select Service - Y1564 Bi-Directional Test form opens.

ii Click on the Search button and choose the VLL Epipe service that you need to test.

iii Click on the OK button. The Y1564 Bi-Directional Test (Create) form reappears with the service information and additional panels.

31 Configure the Source Site and SAP.

i In the Source Site panel, click on the Select button. The Select Source Site - Y1564 Bi-Directional Test form opens.

ii Click on the Search button and choose the 7210 SAS site that contains the source endpoint of the Epipe service.

iii Click on the OK button. The Y1564 Bi-Directional Test (Create) form reappears with the Source Site information and additional panels.

iv In the Source Test SAP section of the Source SAPs panel, click on the Select button. The Select Source Test SAP - Y1564 Bi-Directional Test form opens.

v Click on the Search button and choose the port that contains the source SAP for the Epipe service.

vi Click on the OK button. The Y1564 Bi-Directional Test (Create) form reappears with the Source Test SAP information displayed.

32 Configure the Remote Site and SAP, if required.



Note — Configuration of the Remote Site and SAP is optional in an Epipe service, since the second endpoint becomes the remote site and SAP by default. However, you must perform this step if you need to select a Remote SAP Target Port in order to move SAPs. See step 34.

i In the Remote Site panel, click on the Select button. The Select Remote Site - Y1564 Bi-Directional Test form opens.

ii Click on the Search button and choose the site that contains the remote endpoint of the Epipe service.

iii Click on the OK button. The Y1564 Bi-Directional Test (Create) form reappears with the Remote Site information displayed.

iv In the Remote Test SAP section of the Remote SAPs panel, click on the Select button. The Select Remote Test SAP - Y1564 Bi-Directional Test form opens.

v Click on the Search button and choose the port that contains the remote SAP for the Epipe service.

vi Click on the OK button. The Y1564 Bi-Directional Test (Create) form reappears with the Remote SAP information displayed.

33 Configure the Forwarding Class parameter, if required.

34 If required, move the SAPs to prevent service disruptions.



Note — When the ports that contain the source SAP or remote SAP also contain SAPs for services other than the service you are testing, the test may have an impact on those other services. If this impact is not a concern, you can enable the Ignore Service Impact Validations parameter. If service impact is a concern, you can choose to move the test source SAP or remote SAP to other ports that will not have an impact on services. When you move SAPs, leave the Ignore Service Impact Validations check box unselected. See Chapter 81 for more information.

i If service impact is not a concern, enable the Ignore Service Impact Validations parameter and go to step 35. Otherwise, go to step ii.

ii If required, click on the Select button in the Target Port section of the Source SAPs panel. The Select Target Port - Y1564 Bi-Directional Test form opens.

iii Click on the Search button and choose a port from the list that does not have an associated service.

iv Click on the OK button. The Y1564 Bi-Directional Test (Create) form reappears with the Target Port name displayed.

v If required, click on the Select button in the Target Port for Remote SAP section of the Remote SAPs panel. The Select Target Port for Remote SAP- Y1564 Bi-Directional Test form opens.

vi Click on the Search button and choose a port from the list that does not have an associated service.

vii Click on the OK button. The Y1564 Bi-Directional Test (Create) form reappears with the Target Port for Remote SAP name displayed.

35 Associate a test-head profile with the test.

i Click on the Test Parameters tab.

ii In the Profile panel, click on the Select button. The Select Profile - Y1564 Bi-Directional Test form opens.

iii Click on the Search button and choose a profile from the list. The Y1564 Bi-Directional Test (Create) form reappears with the profile information and additional panels.



Note — Alternatively, you can create a new test-head profile. See "Create a test-head profile" in this section.

iv Click on the Select button in the Payload section of the Payload and Acceptance Criteria panel. The Select Payload - Y1564 Bi-Directional Test form opens.

v Click on the Search button and choose a Frame Payload configuration from the list.

vi Click on the OK button. The Y1564 Bi-Directional Test (Create) form reappears with the Payload information, and the OK and Apply buttons are activated.

vii If required, click on the Select button in the Acceptance Criteria section of the Payload and Acceptance Criteria panel. Otherwise, go to step x. The select Acceptance Criteria - Y1564 Bi-Directional Test form opens.

viii Click on the Search button and choose an Acceptance Criteria configuration from the list.

ix Click on the OK button. The Y1564 Bi-Directional Test (Create) form reappears with the Acceptance Criteria ID displayed.

x Click on the Apply button.

36 If you configured a target port to perform a SAP move in step 34, click on the General tab and go to step 37. Otherwise, go to step 39 to execute the test.

37 Click on the Apply button. The Prepare and Execute buttons are activated.

38 Click on the Prepare button. The Source Test SAP and Remote Test SAP are moved to the Target ports. See Chapter 81 for more information.

39 Click on the Execute button to execute the test. The results tab of the Y1564 Bi-Directional Test is displayed. The test appears in the list.

40 Click on the test in the list to view the results. The Y1564 Bi-Directional Test - Results (View) form opens. The Result Status field displays Pending… until the test is complete. The test duration is configured in the test profile, and is displayed in the Test Duration panel. When the test is complete, the test information is displayed

41 To restore the moved SAPs to their original ports, click on the General tab and then click on the Restore button. See Procedure 81-2.

77.11 Sample OmniSwitch device SLA testing

You can use the 5620 SAM STM to perform a CPE SLA Test-Head OAM test to validate and test customer SLAs used on select OmniSwitch devices in Metro Ethernet networks. The test is critical for provisioning or troubleshooting network services between customer endpoints. The CPE SLA Test-Head OAM test supports unidirectional traffic and IPv4.

You can perform the following tasks on the 5620 SAM without an external test-head device:

- Generate specific flow-based traffic across the network to help identify flow-based issues.
- Identify the impact of QoS settings (for example, SAP profile or QoS policies) on the overall traffic.
- Check the throughput across a provider network. The throughput is displayed on the 5620 SAM GUI for each iteration of the test.
- Debug flow-specific traffic forwarding across the provider network.
- Analyze the behavior of various user-defined traffic patterns across the provider network.
- Perform the handover testing after the initial deployment.
- Perform on-demand testing and results monitoring using a central entity.

You can perform a CPE SLA Test-Head test using one CPE test-head profile or a group of profiles. You can also run several tests for one CPE Test-Head profile or group of profiles.

The following conditions are applicable to the creation of a CPE SLA Test-Head profile or a group of profiles and their execution:

- A CPE SLA Test-Head Group profile can contain up to eight stream/flows.
- A CPE SLA Test-Head Group profile can contain up to eight analyzers.
- When you configure the STM test execution details, the analyzer test name and the generator test name must be the same.
- If the analyzer has a test (flow) which is not in the generator group profile, the test is not valid.
- When you run a CPE SLA test or test group, only one test can be run at a time. You cannot run concurrent tests on the same device.

The following steps describe how to create a CPE SLA Test-Head profile or a group of profiles on the following devices:

- OS 6250M (Metro)
- OS 6250SME (Enterprise) with Metro license
- OS 6400
- OS 6450 with Metro license
- OS 6850E
- OS 6855 U24X
- OS 9000E



Note — This functionality is available for OS 6400, OS 6850E, OS 6855 U24X, and OS 9000E NEs with Release 6.4.5 R02 and later. For these NEs, CPE SLA Test-Head profiles and CPE SLA Test-Head Group profiles will be for distribution only if the profile has a Tx Rate of 64kbps or above.

The procedure lists only the configuration steps and parameters that are required for the sample. See the procedures in section 77.13 for complete STM configuration information.

Create a CPE SLA Test-Head profile

1 Choose Tools→AOS CPE Test-Head Profiles→CPE Test-Head Profile from the 5620 SAM main menu. The CPE Test-Head Profiles form opens.

2 Click on the Create button. The CPE Test-Head Profile, Global Policy (Create) form opens.

3 Configure the following parameters:

- Name
- Description
- Source Endpoint
- Destination Endpoint
- Source MAC
- Destination MAC
- Direction
- Role
- Tx Rate (kbps)
- Frame Size (bytes)

4 Configure the Frame Type parameter. The CPE Test-Head Profile, Global Policy (Create) form refreshes and displays additional parameters.

5 Configure the following parameters:

- VLAN-Tag
- Priority
- Pattern
- Drop Enable

6 Perform one of the following:

a If you set the Frame Type parameter to Ethernet, configure the Ether Type parameter.

b If you set the Frame Type parameter to IPV4, configure the following parameters.

- Source IP
- Destination IP
- Protocol
- TOS
- TTL
- Source Port
- Destination Port

The Source Port and Destination Port parameters appear when you set the Protocol parameter to TCP or UDP.

7 Click on the OK button. The CPE Test-Head Profiles form opens.

8 Click on the Search button to display the CPE Test-Head profile.

9 Choose the CPE Test-Head profile and click on the Released button to change the Global policy configuration mode to Released. Acknowledge the Warning message as required. You must release each CPE Test-Head test profile separately.

10 Distribute the CPE Test-Head profile locally to the managed devices.



Note — Policies are also automatically distributed to devices when the policies are used by resources on the device. See chapter 42 for more information about policies and policy distribution.

i Choose the CPE Test-Head profile and click on the Distribute button. The Distribute - CPE Test Head Profile form opens.

ii Choose the appropriate nodes from the Available Nodes column and click on the Move-right button.

iii Click on the Distribute button and close the form.

11 Configure the VLAN and port settings for the CPE Test-Head profile.

i Choose the CPE Test-Head profile and click on the Properties button to view the profile parameter settings.

ii Click on the Local Definitions tab and click on the Search button. The devices to which the test policy was distributed in step 10 appear.

iii Choose a device from the list and click on the Properties button. The CPE Test-Head Profile form opens with the General tab displayed.

iv In the VLAN panel, click on the Select button for the Service ID parameter. The Select vlanSitePointer - CPE Test-Head Profile form opens.

v Click on the Search button to list the VLAN sites.

vi Choose a device and click on the OK button.

vii Click on the Local Audit On button to change the mode to Local Edit only.

viii Click on the Select button for the Port parameter. The Select vlan port - CPE Test-Head Profile form opens.

ix Click on the Search button to list the ports.

x Choose a port and click on the OK button.

xi Click on the Apply button and close the form.

12 As required, repeat steps 1 to 11 if you need to create additional CPE SLA Test-Head profiles. You can group profiles as described in step 13, otherwise, go to step 15.

Create a CPE SLA Test-Head Group profile

13 If required, create a CPE SLA Test-Head Group profile which can be use to bind individual CPE Test-Head profiles to form a group of tests.

i Choose Tools→AOS CPE Test-Head Profiles→CPE Test-Head Group Profile from the 5620 SAM main menu. The CPE Test-Head Group Profile form opens.

ii Click on the Create button. The CPE Test-Head Group Profile, Global Policy (Create) form opens.

iii Configure the following parameters:

- Name
- Description
- Source Endpoint
- Destination Endpoint
- Direction
- Role
- Tx Rate (kbps)



Note — If the Role parameter is set to the Generator option, perform step 14 otherwise, continue with step 13.

iv Click on the CPE Test Group Member tab and click on the Create button. The Select Port - CPE Test Group Profile - Global Policy forms opens.

v Choose the appropriate CPE Test-Head profiles from the list and click on the OK button. The CPE Test-Head Group Profile, Global Policy (Create) form opens displaying the selected profiles.

vi Click on the OK button to save CPE Test-Head Group profile.

vii Click on the Search button to display the CPE Test-Head Group profile.

viii Choose the CPE Test-Head Group profile and perform steps 9, 10, and 11.

ix Go to step 15.

14 Configure the required feeder port for the generator.

i On the 5620 SAM network topology map, right-click on the appropriate device and choose Properties from the contextual menu. The Network Element - <*Node Name*> (Edit) form appears.

ii Click on the Globals tab.

iii Click on the AOS OAM tab.

iv Click on the Select button that is associated with the Feeder Port Name parameter. The Select Feeder Port - Network Element - <*Node Name*> form appears.

v Click on the Search button to list the feeder ports.

vi Choose the appropriate feeder port and click on the OK button. The Network Element - <*Node Name*> (Edit) form reappears.

vii Click on the OK button to save the feeder port information.

viii Perform the rest of the substeps in step 13.

Configure the STM test execution details

15 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager (STM) form opens.

16 Click on the Create button and choose one of the following options:

a AOS CPE→CPE SLA Test—Allows you to run a test on a CPE test-head profile or a group of profiles. The CPE SLA Test, CPETest-0 (Create) form opens with the General tab displayed. Perform steps 17 to 20, and step 22 to configure this option.

b AOS CPE→CPE SLA Test Group—Allows you to run several tests on a on a CPE test-head profile or group of profiles. The CPE SLA Test Group, CPETest-0 (Create) form opens with the General tab displayed. Complete steps 17, 18, 20, 21, and step 22 to configure this option.

17 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State

18 In the Generator panel, click on the Select button. The Select Generator - CPE SLA Test - CPET Test-0 form opens.

i Click on the Search button to list the generator profiles.

ii Choose a generator profile and click on the OK button to close the form.

19 In the Analyzer panel, click on the Select button. The Select Analyzer - CPE SLA Test - CPET Test-0 form opens.

i Click on the Search button to list the analyzer profiles.

ii Choose an analyzer profile and click on the OK button to close the form.

20 Click on the Test Parameters tab and configure the following parameters:

- Number of Test Iterations
- Test Iteration Duration
- Generator Tx Rate
- Generator Frame Size (bytes)
- Increase Tx Rate Every Iteration

21 Click on the CPE SLA Test Group Members tab and click on the Create button. The CPE Test-Head Group Profile - CPE SLA Test Group CPETestGroup - 0 forms opens.

i Click on the Search button to display the CPE Test-Head Group profiles.

ii Choose the appropriate CPE Test-Head Group profiles and click on the OK button to close the form. The CPE SLA Test Group, CPETest-0 (Create) form reappears.

22 Click on the OK button to close the form.

Run the STM test and analyze the results

23 In the Service Test Manager (STM) form, choose one of the following options from the Test (Assurance) drop-down menu and click on the Search button.

a CPE SLA Test (AOS SAS)—This option displays all single CPE test-head profile tests that have been created.

b CPE SLA Test Group (AOS SAS)—This option displays all group CPE test-head profile tests that have been created.

24 Choose the appropriate CPE SLA test and click on the Execute button to start the test.

25 To view the test results, click on the Results tab.

77.12 Workflow to use the Service Test Manager

1 If you are configuring an OAM or an Ethernet CFM test, review the appropriate workflow.

a Review "Workflow to use OAM diagnostic tests" in chapter 32.

b Review "Workflow to configure Ethernet CFM" in chapter 78.

2 As required, configure the STM default settings to meet your operational requirements:

a Customize the STM default system preferences such as the default retention time for db test results and log file. See the *5620 SAM System Administrator Guide* for more information.

b Enable the debug STM mode, which allows you to access more options on the STM form. See Procedure 3-19 for more information.

3 Create or modify an STM test policy to define the generated tests for the STM test suite. See Procedure 77-1 for more information.

4 As required, configure the threshold-crossing alarms for test policies, test definitions, and assurance tests.

a Configure threshold-crossing alarms on NE-schedulable OAM tests within a test policy. See Procedure 77-2 for more information.

b Configure threshold-crossing alarms on non-NE-schedulable OAM tests within a test policy. See Procedure 77-3 for more information.

5 Create or modify an STM test suite. See Procedure 77-4 or 77-5 for more information.

- Choose the type of entity to which the suite applies.
  - Choose None if you want to include tests that are associated with different types of entities, such as VLL and Tunnel (SDP).
- As required:
  - associate a test policy with the test suite
  - choose tests for the first-run test group
  - generate tests for the test suite
  - choose tests for the last-run test group

6 As required, create a schedule for an STM test suite that you want to execute regularly for continual network monitoring. To schedule the execution of a test suite, you must first create the SAM schedule. See chapter 7 for information about creating schedules.

a Schedule the execution of a test suite using a SAM schedule. See Procedure 77-6 for more information.

b Configure threshold-crossing alarms on non-NE-schedulable OAM tests within a test policy. See Procedure 77-7 for more information.

c Enable the scheduled tasks.

d Apply schedules to test suites as required to create scheduled tasks.

7 Execute the STM test suite. See Procedure 77-8 more information.

8 Execute individual or multiple tests from the STM. See Procedure 77-10 more information.

9 Monitor the diagnostic results from the scheduled test suites and the alarm list for indications of network or service faults and threshold-crossing alarms.

a View test suite results. See Procedure 77-11 for more information.

b View and compare test suite results for a tested entity. See Procedure 77-12 for more information.

c View and compare test results. See Procedure 77-13 for more information.

77.13 Service Test Manager procedures

The following procedures describe how to perform 5620 SAM STM tasks.

Procedure 77-1 To configure a STM test policy

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Perform one of the following:

a Create a test policy. Perform the following steps.

i Click on the Create button.

ii Choose Test Policy from the Create contextual menu. The Test Policy (Create) form opens with the General tab displayed.

iii Configure the parameters:

- ID
- Auto-Assign ID
- NE Schedulable
- Entity Type
- Accounting Files
- Continuously Executed
- Test Result Storage

The Accounting Files, Continuously Executed, and Test Result Storage parameters are configurable when the NE Schedulable parameter is enabled.

The Continuously Executed and Test Result Storage parameters are only configurable when the Accounting Files parameter is enabled.

iv Go to step 3.



Note 1 — You must enable the NE Schedulable parameter if the test suite that you create using the policy is to become an NE scheduled task.

Note 2 — If you are creating a CFM Ethernet test, you must enable the NE Schedulable parameter, and optionally you can configure the Accounting Files and Continuously Executed parameters. You must select VLL Service, VPLS, or Composite Service for the Entity Type parameter.

b Configure an existing policy. Perform the following steps.



Note — If you modify a test policy that is associated with a test suite, you must regenerate the Generated tests in the test suite.

i Choose Test Policy (Assurance) from the object drop-down list.

ii Configure the filter criteria, if required, and click on the Search button. A list of test policies appears.

iii Choose a test policy and click on the Properties button. The Test Policy (Edit) form opens with the General tab displayed.

3 Configure the parameters:

- Name
- Description
- Strategy

The Strategy parameter is only configurable when the Entity Type parameter is set to VLL Services.

4 Click on the Test Definitions tab.

5 Click on the Add button to add a test definition to the test policy. A cascading submenu appears.

6 Choose an option from one of the categories in the cascading submenu. The options that appear depend on the Entity Type and NE Schedulable parameter values you specified in step 3. For example, Ethernet CFM test definition options only appears if you selected either the VLL Service or VPLS option as the Entity Type and if you also enabled the NE Schedulable parameter.

Each option in this step has three tabs that contain configurable parameters: General, Test Parameters, and Results Configuration. Parameters that are common to all options are listed in the remainder of this step. Parameters that are specific to a particular option are configured in step 7.

The following configurable parameters appear on the General tab of the configuration form for every option:

- Name
- Description
- Administrative State

Some or all of the following configurable parameters appear on the Test Parameters tab of the configuration form for most options in this step:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Probe History
- Forwarding Class
- Forwarding Profile

The Probe History parameter is configurable when the NE Schedulable parameter is enabled.

A combination of the following configurable parameters appears on the Results Configuration tab of the configuration form for most options in this step:

- Probe History Size (rows)
- Test Failure Threshold
- Packet Failure Threshold
- Maximum Failures
- Trap Generation

7 Perform this step to configure the parameters that are specific to the particular test definition you are creating.

Choose the required test definition option from the following:

a Site ping test definition (Service→Add Site Ping) for a VLL service, VPLS, VPRN service, mirror service, service connector, or router:

i Click on the Test Parameters tab.

ii Configure the parameters:

- Use Local Tunnel
- Use Remote Tunnel

iii Go to step 8.

b VCCV ping test definition (Service→Add VCCV Ping) for a VPLS/MVPLS/HVPLS or VLL service:

i Click on the Test Parameters tab.

ii Configure the parameters:

- Size (octets)
- Forwarding Class
- Forwarding Profile
- Reply Type

iii Go to step 8.

c VCCV trace test definition (Service→Add VCCV Trace) for a VLL service:

i Click on the Test Parameters tab.

ii Configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Size (octets)
- Forwarding Class
- Forwarding Profile
- Reply Type

iii Go to step 8.

d MAC ping test definition (Service→Add MAC Ping) for a VLL service or VPLS:

i Configure the following parameters on the General tab:

- Target MAC Address
- Source MAC Address

ii Click on the Test Parameters tab.

iii Configure the parameters:

- Time To Live
- Forwarding Class
- Forwarding Profile
- Reply Control
- Control Plane

iv Go to step 8.

e Multicast FIB ping test definition (Multicast→Add MFIB Ping) for a VPLS:

i Configure the following additional parameters on the General tab:

- Multicast Source
- Multicast Group

ii Click on the Test Parameters tab.

iii Configure the parameters:

- Time To Live
- Reply Via Control Plane

iv Go to step 8.

f Ping test definition (L3 Service→Add VPRN Ping) for a VPRN:

i Click on the Test Parameters tab.

ii Configure the parameters:

- Time To Live
- Reply Via Control Plane

iii Go to step 8.

g Trace test definition (L3 Service→Add VPRN Trace) for a VPRN:

i Click on the Test Parameters tab.

ii Configure the parameters:

- Initial Time to Live
- Maximum Time to Live
- DiffServ Field
- Reply Via Control Plane

iii Go to step 8.

h Multicast routing information test definition (Multicast→Add mrinfo) for a VPRN or router:

i There are no parameters that are specific to the mrinfo test definition.

ii Go to step 8.

i Multicast trace test definition (Multicast→Add mtrace) for a VPRN or router:

i Click on the Select button on the General tab to choose a multicast group to run the trace against.

ii Click on the Test Parameters tab.

iii Configure the parameters:

- Initial Time to Live
- Maximum Number of Hops

iv Go to step 8.

j ICMP ping test definition (ICMP→Add ICMP Ping) for a VPRN or router:

i Click on the Test Parameters tab.

ii Configure the parameters:

- Size (octets)
- Rapid
- Time To Live
- Data Pattern
- Positional Data Pattern
- DiffServ Field
- Bypass Routing
- Do Not Fragment
- Forwarding Class
- Forwarding Profile

iii Go to step 8.

k ICMP trace test definition (ICMP→Add ICMP Trace) for a VPRN or router:

i Click on the Test Parameters tab.

ii Configure the parameters:

- DiffServ Field
- Time To Wait (milliseconds)

iii Go to step 8.

l Tunnel ping test definition (Service Transport→Add Tunnel Ping) for a service tunnel:

i Click on the Test Parameters tab.

ii Configure the parameters:

- Size (octets)
- Forwarding Class
- Forwarding Profile

iii Go to step 8.

m MTU ping test definition (Service Transport→Add MTU Ping) for a service tunnel:

i Click on the Test Parameters tab.

ii Configure the parameters:

- Size (octets)
- MTU Start Size (octets)
- MTU End Size (octets)
- MTU Step Size (octets)

iii Go to step 8.

n Ping test definition (MPLS→Add LSP Ping) for an LSP:

i In the General tab, configure the Target Type parameter. If you are adding an MPLS-TP LSP ping test definition, go to step o.

ii Click on the Test Parameters tab.

iii Configure the parameters:

- Size (octets)
- Time To Live
- Forwarding Class
- Forwarding Profile

iv Go to step 8.

o Ping test definition (MPLS→Add LSP Ping) for an MPLS-TP LSP:



Note — The Entity Type parameter in step 2 must be set to LSP (MPLS-TP).

i Click on the Test Parameters tab.

ii Configure the parameters in the Execution Details panel:

- Number of Test Probes
- Packet Interval (seconds)
- Probe Timeout (seconds)

iii Configure the parameters in the Test Probe panel:

- Size (octets)
- Time To Live
- Forwarding Class
- Forwarding Profile

iv Go to step 8.

p Trace test definition (MPLS→Add LSP Trace) for an LSP:

i In the General tab, configure the Target Type parameter. If you are adding an MPLS-TP LSP ping test definition, go to step q

ii Click on the Test Parameters tab.

iii Configure the parameters:

- Size (octets)
- Initial Time to Live
- Maximum Time to Live
- Forwarding Class
- Forwarding Profile

iv Go to step 8.

q Trace test definition (MPLS→Add LSP Trace) for an MPLS-TP LSP:



Note — The Entity Type parameter in step 2 must be set to LSP (MPLS-TP).

i Click on the Test Parameters tab.

ii Configure the parameters in the Execution Details panel:

- Number of Test Probes
- Packet Interval (seconds)
- Probe Timeout (seconds)

iii Configure the parameters in the Test Probe panel:

- Size (octets)
- Initial Time To Live
- Maximum Time To Live
- Forwarding Class
- Forwarding Profile

iv Go to step 8.

r Ping test definition (MPLS→Add P2MP LSP Ping) for a P2MP LSP or P2MP LDP:

i Click on the Test Parameters tab.

ii Configure the parameters:

- Packet Timeout (seconds)
- Packet Interval (seconds)
- Size (octets)
- Time To Live
- Forwarding Class
- Forwarding Profile

The Time To Live parameter is only displayed when the Entity Type parameter is set to P2MP LSP.

iii Go to step 8.

s Trace test definition (MPLS→Add P2MP LSP Trace) for a P2MP LSP:

i Click on the Test Parameters tab.

ii Configure the parameters:

- Size (octets)
- Initial Time to Live
- Maximum Time to Live
- Forwarding Class
- Forwarding Profile

iii Go to step 8.

t Ping test definition (L1/L2→Add ATM Ping) for an ATM PVC:

i Click on the Test Parameters tab.

ii Configure the parameters:

- Loopback Location (hex)
- Destination Type

iii Go to step 8.

u CFM loopback test definition (Ethernet CFM→Add CFM Loopback) for a VLL service or VPLS:

i Click on the Test Parameters tab.

ii Configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Forwarding Class
- Forwarding Profile
- Size (octets)

iii Go to step 8.

v CFM link trace test definition (Ethernet CFM→Add CFM Link Trace) for a VLL service or VPLS:



Note — Creating a CFM link trace test policy with the Continuously Executed parameter enabled can create a large number of results, and cause a long delay when deleting the test suite. Alcatel-Lucent recommends that you disable the Continuously Executed parameter for test suites that use CFM link trace tests.

i Click on the Test Parameters tab.

ii Configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Forwarding Class
- Forwarding Profile
- TTL

iii Go to step 8.

w CFM two way delay test definition (Ethernet CFM→Add CFM Two Way Delay Test) for a VLL service or VPLS:

i Click on the Test Parameters tab.

ii Configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Forwarding Class
- Forwarding Profile

iii Go to step 8.

x CFM two way SLM test definition (Ethernet CFM→Add CFM Two Way SLM) for a VLL service or VPLS:

i Click on the Test Parameters tab.

ii Configure the parameters:

- Number of Test Packets
- Packet Interval (seconds)
- Packet Timeout (seconds)
- Forwarding Class
- Forwarding Profile
- Size (octets)

iii Go to step 8.

8 To configure threshold-crossing alarms as required, perform the following:

a Click on the Thresholds tab.

b Perform steps 9 to 15 of Procedure 77-3.

9 Click on the OK button. The Definition Create form closes and a dialog box appears.

10 Click on the OK button. The Test Policy (Create|Edit) form reappears with the new OAM test definition listed.

11 Perform steps 4 to 10 to add additional OAM test definitions to the policy.

12 If you added Ethernet CFM test definitions to the test policy then go to step 13. Otherwise go to step 19.

13 Click on the CFM Details tab.

14 Click the Select button to choose a MD Mgr Object ID. The Select Maintenance Domain form is displayed.

15 Click the Search button and choose the required maintenance domain from the list.

16 Click OK. The Select Maintenance Domain form closes and the selected MD Mgr Object ID is displayed in the CFM Details tab.

17 If you are configuring an existing test policy, click on the Update Test Suites button to apply the test policy changes to all test suites that are associated with the test policy. If you are creating a test policy, go to step 19.



Caution — The operation of scheduled test suites that use the test policy may be adversely affected if you modify the test policy while a scheduled task for the suite is enabled.

18 Click on the Usages tab to view a list of the test suites that use the test policy.

19 Click on the OK button. The Test Policy (Create|Edit) form closes.

20 Close the Service Test Manager form.

Procedure 77-2 To configure threshold-crossing alarms on NE-schedulable OAM tests within a test policy

Perform this procedure to configure threshold-crossing alarms for test policies, test definitions, and assurance tests that are NE-schedulable. An alarm is raised when a threshold is crossed, either because the value rose above or fell below the configured level.

Configuring threshold-crossing alarms on a test definition within the test policy creates a threshold definition that applies to generated tests. Configuring threshold-crossing alarms directly on a test that is NE-schedulable applies just to the test.



Note — If you modify a test policy associated with a test suite, you must regenerate the generated tests in the test suite.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose Test Policy (Assurance) from the object drop-down list.

3 Configure the filter criteria, if required, and click on the Search button. A list of test policies is displayed.

4 Choose an NE-schedulable policy from the list and click on the Properties button. The Test Policy (Edit) form opens with the General tab displayed.

5 Click on the Test Definitions tab. A list of tests associated with the policy opens.

6 Select a test from the list and click on the Properties button. The Test Definition—Test Policy (Edit) form opens with the General tab displayed.

7 Click on the Thresholds tab.

8 Click on the Create button. The Threshold Event Definition (Create) form opens with the General tab displayed.

9 Configure the parameters:

- Type
- Generate Alarm on Rising Threshold
- Clear Alarm on Falling Threshold
- Update Test Result Status
- Include Falling Threshold

The Clear Alarm on Falling Threshold parameter is configurable only when you enable the Include Falling Threshold parameter.

10 Click on the Rising Threshold tab.

11 Configure the Threshold Value parameter.

12 Click on the Falling Threshold tab.



Note — The Falling Threshold tab can be accessed only when the Include Falling Threshold parameter is enabled on the General tab of the Threshold Event Definition (Create) form.

13 Configure the Threshold Value parameter.

14 Click on the OK button. The Threshold Event Definition (Create) form closes and a dialog box appears.

15 Click on the OK button. The test appears on the list.

16 Repeat steps 8 to 15 to configure threshold events on additional tests.

17 Click on the OK button. The Test Definition—Test Policy (Edit) form closes and the Test Policy (Edit) form reappears.

18 Click on the OK button. A dialog box appears.

19 Confirm the action. The Test Policy (Edit) form closes and the Service Test Manager form reappears.

20 Close the Service Test Manager form.

Procedure 77-3 To configure threshold-crossing alarms on non-NE-schedulable OAM tests within a test policy

You can configure threshold-crossing alarms for test policies, test definitions, and assurance tests that are non-NE-schedulable. An alarm is raised when a threshold is crossed, either because the value rose above or fell below the configured level.

Configuring threshold-crossing alarms on a test definition within the test policy creates a threshold definition that applies to generated tests. Configuring threshold-crossing alarms directly on a test that is non-NE-schedulable applies just to the test.



Note — If you modify a test policy associated with a test suite, you must regenerate the generated tests in the test suite.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose Test Policy (Assurance) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of test policies is displayed.

5 Choose a non-NE-schedulable policy from the list and click on the Properties button. The Test Policy (Edit) form opens with the General tab displayed.

6 Click on the Test Definitions tab. A list of tests associated with the policy opens.

7 Select a test from the list and click on the Properties button. The Test Definition—Test Policy (Edit) form opens with the General tab displayed.

8 Click on the Thresholds tab.



Note — The Thresholds tab is enabled or disabled depending on the test type selected in step 7. Threshold alarm events can not be configured for Site Ping, mrinfo, mtrace, VPRN Trace and Mtu Ping tests.

9 Click on the Create button. The Threshold Event Definition (Create) form opens with the General tab displayed.

10 Configure the parameters.

- Type
- Generate Alarm on Rising Threshold
- Clear Alarm on Falling Threshold
- Update Test Result Status
- Include Falling Threshold

The Clear Alarm on Falling Threshold parameter is configurable only when you enable the Include Falling Threshold parameter.

11 Click on the Rising Threshold tab.

12 Configure the Threshold Value parameter.

13 Click on the Falling Threshold tab.



Note — The Falling Threshold tab can be accessed only when the Include Falling Threshold parameter is enabled on the General tab of the Threshold Event Definition (Create) form.

14 Configure the Threshold Value parameter.

15 Click on the OK button. The Threshold Event Definition, (Create) form closes and a dialog box appears.

16 Click on the OK button. The test appears on the list.

17 Repeat steps 9 to 16 to configure threshold events on additional tests in the policy.

18 Click on the OK button. The Test Definition, Test Policy (Edit) form closes and the Test Policy (Edit) form reappears.

19 Click on the OK button. A dialog box appears.

20 Confirm the action. The Test Policy (Edit) form closes and the Service Test Manager form reappears.

21 Close the Service Test Manager form.

Procedure 77-4 To create a test suite

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Test Suite from the contextual menu. The Test Suite (Create) form opens.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- NE Schedulable
- Entity Type
- Validation Test Suite
- Timeout (minutes)
- First Run Execution Sequence
- Last Run Execution Sequence



Note 1 — The Entity Type parameter specifies that only test policies created for the same entity type are available for the test suite. The parameter also restricts the predefined tests that are available as first-run or last-run tests to those that apply to the entity type.

Note 2 — To create a test suite that includes tests for different entity types, specify None as the Entity Type parameter value. This allows you to choose any predefined test as a first-run or last-run test.

Note 3 — Specifying None as the Entity Type parameter value disables the generation of tests in a test suite; the policy that STM uses to generate tests must be associated with a specific entity type.

Note 4 — The Validation Test Suite parameter specifies that the test suite is used to validate the connectivity of the tested service entity to which it is applied. This is also refered to as a validator test suite. OAM validation tests are not supported for HVPLS.

You must click on the Validate button on the associated service or service tunnel configuration form to run the OAM validator test suite. If the Validate button is not visible, click on the More Actions button and choose Validate. The result of this OAM validation is indicated by the OAM Validation Failed operational flag.

Note 5 — First Run and Last Run tests can be added for test suites that have the Continuously Executed and Accounting Files options enabled can be added to test suites.

Note 6 — When issuing an Execute or Stop command for a test suite that has the Continuously Executed and Accounting Files options enabled, the execution or stopping of the First Run and Last Run tests will be triggered.

Note 7 — If you are creating an Ethernet CFM test suite, you must enable the NE Schedulable parameter.

5 To create a scheduled task, see procedure 77-6.

6 If you chose None as the Entity Type parameter value in step 4, go to step 17. To create a scheduled task, go to step 7.

7 Click on the Test Policy tab.

8 Click on the Add button to choose a test policy to associate with the test suite. The Select Test Policy - Test Suite form opens.

9 Click on the Search button to display a list of available test policies.



Note — Only test policies that apply to the type of entity specified by the Entity Type parameter in step 4 appear in the list.

10 Choose a test policy from the list and click on the OK button. The test policy appears on the Test Policy tab.

11 Click on the Tested Entities tab.

12 Click on the Add button to choose a service, transport element, or device as the object against which the test suite is run. The Add form opens.

13 Click on the Search button to display a list of available entities.



Note 1 — Only entities that match the type of entity specified in the test policy appear in the list.

Note 2 — There is a column titled Test Suite Count in the Search form. This indicates the number of configured test suites that a specific test entity is currently associated with. The counter also includes test suites that do not contain generated tests.

A Test Suite Count indicator is also displayed on the General tab of managed STM test entity objects. These include services, composite services, transport elements, and applicable devices.

14 Choose an entity from the list and click on the OK button. The Add form closes and an entry for the entity appears in the list on the Tested Entities tab.

15 Ensure the item is selected in the list and click on the Lock Test Generation button, if required.



Note — Locking the test generation means that the initial settings you specify when creating the test suite will be retained, even if later on you change some attributes (for instance, if you are testing SDP tunnels and you extend the tested entities by selecting another SDP tunnel). All customized test attributes are retained when re-generating the tests.

The 5620 SAM auto-locks tested entities when generated tests are either modified or deleted.

The Test Re-generation locked field in the list displays a check mark to indicate that the lock is enabled and the button's name changes to Unlock Test Generation. If you do not want to lock the test, then click the Unlock Test Generation button. The Test Re-generation locked field in the list will not display a check mark.

16 Repeat steps 12 to 14 for each additional entity that you want to specify.

17 Click on the First Run Tests tab.

18 Click on the Add button to choose a predefined test that is to execute before the generated tests in the suite. The Add form opens.

19 Click on the Search button to display a list of available tests.

20 Choose a test from the list and click on the OK button. The Add form closes and the test entry appears on the First Run Tests tab.

21 Repeat steps 18 to 20 for each additional first-run test that you want to specify.

22 When there is more than one test in the first-run list, the Move Up and Move Down buttons are active. Select a test entry and click on these buttons as needed to reorder the first-run test execution sequence, if required.

23 Click on the Last Run Tests tab.

24 Click on the Add button to include a predefined test that is to execute after the other tests in the suite have completed. The Add form opens.

25 Click on the Search button to display a list of available tests.

26 Choose a test from the list and click on the OK button. The Add form closes and the test entry appears on the Last Run Tests tab.

27 Repeat steps 24 to 26 for each additional last-run test that you want to specify.

28 When there is more than one test in the last-run list, the Move Up and Move Down buttons are active. Select a test entry and click on these buttons as needed to reorder the last-run test execution sequence, if required.

29 Click on the Apply button to save the changes. Additional buttons at the bottom of the form become active.

30 If you chose None as the Entity Type parameter value in step 4, go to step 34.

31 Click on the Generated Tests tab.

32 Click on the Generate Tests button. The 5620 SAM begins generating tests for the test suite based on the test policy. The tests appear in a list on the Generated Tests form as they are generated.



Note 1 — When the test policy or the configuration of an entity on the Tested Entities tab changes, you must regenerate the tests in the test suite by clicking on the Generate Tests button.

Note 2 — When tests have been generated in a test suite (which has a test policy already associated to it), these existing tests will not be altered (delete and recreated, or set to default tests), when the Generate Tests button is pressed again.

Note 3 — Any of the tests generated by a test suite can be deleted directly from the list on the Generated Tests tab. Select the tests you want to delete and press the Delete button.

Note 4 — For a test suite containing a P2MP LSP Ping Test Policy, the test suite generator will generate one test per S2L path (for P2MP LSP) or one test per leaf node address (for P2MP LDP).

33 Click on the Generation Logs tab to view the log file that the 5620 SAM creates during test generation, as required.



Note — Generation Logs messages only appear if any failures occur during the test generation process.

34 Click on the OK button to close the Test Suite (Create) form.

35 Close the Service Test Manager form.

Procedure 77-5 To modify a test suite

1 You can modify an existing test suite in two different ways. Perform one of the following:

   a Modify the test suite from within the Service Test Manager. Go to step 2.

   b Modify the test suite from within a tested entity. Go to step 11.

2 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

3 Choose Test Suite (Assurance) from the object drop-down list.

4 Configure the filter criteria.

5 Click on the Search button. A list of test suites appears.

6 Select a test suite and click on the Properties button. The Test Suite (Edit) form opens with the General tab displayed. Use the parameters on this tab to change the execution order of tests in the First run and Last run test groups, as required.

   The following tabs list the test-suite components that you can individually or collectively add to or remove from the test suite:

   - Test Policy tab — displays the test policy that is associated with the test suite
   - Tested Entities tab — lists the entities that are the subjects of the tests in the test suite
   - First Run Tests tab — lists the group of tests in the test suite that run first
   - Generated Tests tab — lists the generated tests that are included in the test suite
   - Last Run Tests tab — lists the group of tests in the test suite that run last

The following tabs display information about the creation and execution of the test suite:

- Results tab — lists the per-run results that are returned by each execution of the test suite
- Individual Test Results tab — lists all individual test results. This is similar to what is displayed when a Tested Entity is chosen and you click on Show Results.
- Generation Logs tab — lists the log entries that are created during test generation for the test suite
- Faults tab — displays the faults associated with the test suite



Note 1 — Generation Logs messages only appear if any failures occur during the test generation process.

Note 2 — You can use the Quick Filter on the test result tab pages to narrow down and limit the displayed results.

7 Modify the parameters for the test suite, as required.

To configure an item on a tab that contains a list of test suite components, select the item and click on the Properties button.

8 Make the changes you want and then click on the OK button. A dialog box appears.

9 Click on the Yes button to confirm the action. The Test Suite (Edit) form closes and the Service Test Manager form reappears.

10 Click on the Close button to close the Service Test Manager form.

11 You can alternatively add an entity to an existing test suite from within the Properties form of the particular entity. Several object types in 5620 SAM support this capability, including:

- VLL service
- VPLS
- VPRN service
- Composite service
- Mirror service
- Service connector
- ATM PVC
- LSP
- P2MP LSP
- Tunnel (SDP)
- P2MP LDP

12 Open the Properties form of the entity you want to add to a test suite.

13 Click on the Tests tab. The Test Suite sub-tab is displayed.

14 Click the Add button. The Add form appears.

15 Click the Search button to display a list of test suites. Only test suites applicable to this type of entity will be displayed.

16 Select the required test suite and click OK. The Add form closes and selected test suite appears in the Test Suite sub-tab.

The entity has now been added to this test suite. You can confirm this by clicking the Properties button to display the Test Suite (Edit) form. The newly-added entity will appear on the list in the Tested Entities tab. You can also modify any other parameters of the test suite here, as detailed in steps 2 to 9 above.



Note — Once you have added the entity, you can also run the test suite from the Test Suite sub-tab by clicking the Execute button.

Refer to Procedure 77-8 for information on executing a test suite.

Procedure 77-6 To schedule the execution of a test suite

You can use a SAM schedule to schedule the execution of a test suite. See chapter 7 for information about SAM schedules.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose Test Suite (Assurance) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of test suites appears.

5 Double-click on the test suite that you need to schedule. The Test Suite (Edit) form opens with the General tab displayed.

6 Click on the Schedule button. The STM Scheduled Task (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Scheduled Task Name
- Scheduled Task Description
- Administrative State



Caution — Setting the Administrative State parameter to Enabled puts the scheduled task into effect according to the schedule parameters. Ensure that the test suite and the objects to which it applies are appropriately configured before you set the parameter to Enabled.

8 Click on the Select button in the Schedule panel. The Select Schedule - STM Scheduled Task form opens.

9 If required, click on the Create button to configure a new SAM schedule. See Procedure 7-1 for more information.

10 Configure a filter if required and click on the Search button. A list of schedules appears.

11 Choose a schedule and click on the OK button. The Select Schedule - STM Scheduled Task form closes and the identification information for the chosen schedule is displayed on the STM Scheduled Task (Create) form.

12 Click on the OK button. The STM Scheduled Task (Create) form closes and the Test Suite (Edit) form reappears.

13 Close the Test Suite (Edit) form.

14 Close the Service Test Manager form.

Procedure 77-7 To schedule the execution of a test suite using an existing NE schedule

To schedule the execution of a test suite using an existing NE schedule, perform Procedure 7-5 to turn up the NE scheduled task.

Procedure 77-8 To execute a STM test suite

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose Test Suite (Assurance) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of test suites appears.

5 Select a test suite in the list and click on the Properties button. The Test Suite (Edit) form opens with the General tab displayed.

6 Click on the Execute button. Execution of the test suite begins. You can view the test results when the test execution is complete.



Note 1 — You can run an OAM validation test from the Properties form of a service tunnel or an applicable service. See the applicable service management chapter for more information.

Note 2 — When you execute a test suite from the Properties form of an applicable service, only the tests belonging to that service will be executed. Tests within the suite, but not associated with the current tested entity, will not be executed.

Note 3 — When you execute a test suite under the tested entity (using the Execute button under the entity's Tests>Test Suite sub-tab), 5620 SAM will create a Tested Entity Result under the entity's Tests>Tested Entity Result sub-tab.

Note 4 — You can use the Delete All Result button in either the Results tab or the Individual Test Results tabs to remove all listed test results. Alternatively, you can use the Quick Filter on the test result tab pages to narrow down and limit the displayed results. The Delete All Result button will then only delete the filtered results. If no filter condition is specified, then the Delete All Result button will delete all the pages of results, not just the currently displayed page.

If the list under either of these tabs contains more than 1000 entries, only 1000 entries are displayed at a time, with paging available for the remainder. However, the Delete All Result button deletes all pages of results, not just the currently displayed page.

7 Close the Test Suite (Edit) form.

Procedure 77-9 To run a One Time Validation

The One Time Validation function provides a mechanism to quickly test a service or composite service either at the time it is provisioned or when it is already in service. A variety of services and transport components can be tested using this function.

The One Time Validation function operates in much the same way as running a Validator test suite (refer to Section 77.1 for more information), however the temporary objects that are automatically created for this method are deleted upon its completion. These include the test suite, tests, MEGs, and MEPs. No user action is required to do this.

Another significant difference between the two methods is that no results file is created. Instead, all tests and results are stored as archived objects that remain after the One Time Validation is finished. The results can be viewed in the 5620 SAM GUI. Refer to the 5620 SAM-O XML Reference (oneTimeValidate under sas.TestManager) for the required syntax to view the results using OSSI.

Executing a One Time Validation also updates the OAM Validation Failed state field as required, indicating whether or not the validation was successful.

Perform the following steps to run the One Time Validation:

1 Select the required test entity using the appropriate item under the 5620 SAM Manage menu item, and then click the Properties button. The entity's property form opens. Entities that you can test using this function include:

- VLL, VPLS, and VPRN services (Manage→Service→Services)
- Composite services (Manage→Service→Composite Services)
- Dynmaic LSPs (Manage→MPLS→Dynamic LSPs)
- Service tunnels (Manage→Service Tunnels)

2 Click on the One Time Validation button.



Note — If a regular OAM validation is currently running on the selected test entity, the One Time Validation function will not be executed.

The Choose Validator Test Policy form is displayed and lists all test policies that are applicable to the selected test entity.

3 Select the required policy from the list and click OK.



Note — A default read-only test policy (Validation-Default-Policy) is supplied for this purpose. You can copy this policy but not modify it. Modify the cloned copy as required, or you can select a test policy you have previously created (refer to Procedure 77-1 to create a test policy).

The One Time Validation function proceeds after you click the OK button. The automated operations that occur are as follows:

i The One Time Validation test suite is created.

ii The selected test entity is added to the test suite.

iii Any tests, MEGs, and MEPs that are appropriate to the test entity and that are required to run the validation are created.

iv The generated tests are executed.

v The test entity's OAM Validation Failed state indicator is updated as required (a checkmark indicates the OAM validation failed whereas a blank checkbox indicates that the validation succeeded).

vi Test results for each individual test that was created and executed to perform the validation are copied to new test result objects.

vii The test suite, tests, and any required OAM objects that were created to run the validation are deleted.

4 To view the test results, click on the tested entity's Test tab and then on the One Time Validation Result sub-tab.

Note — These archived test results are also available through the STM. They can be viewed by selecting the One Time Validation Result (Assurance) item from the object drop-down list. See Procedure 77-11 for more information.

5 Select one of the test results in the list and click on the Properties button. The One Time Validation Result (Edit) form opens with the General tab displayed.

6 Review the results as required and then close the One Time Validation Result (Edit) form.

Note — The archived test results are not deleted after viewing. They will remain available until manually deleted by the user.

7 Close the tested entity's property form.

Procedure 77-10 To execute one or more individual tests from the STM

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose Test (Assurance) from the object drop-down list.

3 Click on the Search button. A list of tests appears.

4 To execute a single test, go to step 5. To execute multiple tests directly from the STM list, go to step 8.

5 Select a test in the list and click on the Properties button. The Test (Edit) form opens, with the General tab displayed.

6 Click on the Execute button. Execution of the test begins and the Test (Edit) form displays the Results tab. You can view the test results when the test execution is complete.

7 Go to step 11.

8 Select the tests in the list that you want to run.

Note 1 — You can select and execute multiple tests from the test list, with the exception of CCM Tests. If multiple tests including CCM tests are selected, then the Execute button will be disabled.

Note 2 — You cannot modify multiple tests in one pass. If multiple tests are selected, the Properties button will be disabled.

9 Click on the Execute button. Execution of the tests begins.

10 View the results for any individual test once the execution is complete by clicking on the test in the list and then clicking on the Properties button. The Test (Edit) form opens and the results can be viewed on the Results tab.

11 Close the Test Suite (edit) form.

Procedure 77-11 To view Test Suite results

Perform this procedure to view test suite results from the Test Suite Result form.



Note 1 — You can also view the test suite results for an object from the Tests tab of the configuration form for the object.

Note 2 — You can reorder a column in a tabular information view by dragging the column heading to the desired position, then right-clicking on the column heading and choosing Save Table Preferences.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager (STM) form opens.

2 Choose Test Suite Result (Assurance) from the object drop-down list.

3 Click on the Search button. A list of test suite results appears.

4 Select a test suite result and click on the Properties button. The Test Suite Result (View) form opens with the General tab displayed.

5 View the general information and statistics on the General tab.

6 Click on the Results tab to list the test results from the tests in the test suite.

7 Perform one or both of the following:

a Use the horizontal scroll bar at the bottom of the list to view the tabular information on the listed tests.

b Select an entry from the list and click the Properties button.

The result form for the selected test is displayed.

8 Close the Test Suite Result (View) form.

9 Close the Service Test Manager form.

Procedure 77-12 To view and compare Test Suite results for a tested entity

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose Test Suite (Assurance) from the object drop-down menu.

3 Configure the filter criteria.

4 Click on the Search button. A list of test suites appears.

5 Choose a test suite in the list and click on the Properties button. The Test Suite (edit) form opens with the General tab displayed.

6 Click on the Tested Entities tab to view a list of entities tested by the test suite.

7 Choose a tested entity from the list and click on the Show Results button. The Tested Entity (Edit) form opens.

8 Configure the filter criteria.

9 Click on the Search button. A list of test results appears.

10 Choose a test result from the list and click on the Properties button. The result form for the selected test opens.

11 Close the result form.

12 Close the Tested Entity (Edit) form.

13 Close the Test Suite (Edit) form.

14 Close the Service Test Manager (STM) form.

Procedure 77-13 To view and compare test results

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose Test Result (Assurance) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of test results appears.

5 Choose a test result and click on the Properties button to view the properties of the test. The Results form for the selected test type opens.

6 Close the Results form.

7 Close the Service Test Manager (STM) form.

Procedure 77-14 To delete a test suite

1 If the test suite is scheduled, you must remove the scheduled task associated with the test suite before you can delete the test suite. See chapter 7 for more information.

2 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

3 Choose Test Suite (Assurance) from the object drop-down list.

4 Configure the filter criteria.

5 Click on the Search button. A list of test suites appears.

6 Select a test suite in the list and click on the Delete button. A dialog box appears.

7 Click on the Yes button to confirm the action. The test suite is deleted and removed from the list.

8 Click on the Close button to close the Service Test Manager form.

78 — Ethernet CFM

78.1 Ethernet CFM overview *78-2*

78.2 Workflow to configure Ethernet CFM *78-11*

78.3 Ethernet CFM procedures *78-12*

78.1 Ethernet CFM overview

The 5620 SAM Ethernet Connectivity Fault Management, or Ethernet CFM, function is implemented based on the IEEE 802.1ag OAM standard. This standard describes protocols for detecting, isolating, and reporting connectivity faults in an Ethernet network. You can use Ethernet CFM for the following:

- path discovery
- fault detection
- fault isolation
- fault notification

The IEEE 802.1ag OAM standard partitions a network into eight hierarchical levels called maintenance domains, or MDs. An MD is a network, or part of a network, that is provisioned with a set of maintenance entity groups, or MEGs, which are groups of service sites.

MEGs

Typically, a MEG represents one service and consists of a group of maintenance end points, or MEPs. Only one MEG can be associated with a service, but one service can be associated with multiple MEGs. MDs and MEGs are distributed to NEs using 5620 SAM policy distribution.

Within a MEG, MEPs can be sorted into logical groupings called MEG subgroups. A MEG that contains subgroups is called a Global MEG. By default, a Global MEG has one subgroup. MEG subgroups allow you to group managed MEPs and unmanaged remote MEPs so that Ethernet CFM can be directed to a specific area of a system, a MEG subgroup, rather than the entire system.

Ethernet CFM diagnostic tests detect connectivity failures between pairs of local and remote maintenance end points, or MEPs, in a MEG. Each MEP is a reference point that can initiate or terminate one of the following diagnostic tests:

- CFM continuity check
- CFM loopback
- CFM link trace
- CFM Eth test
- CFM two-way delay
- CFM one-way delay
- CFM single-ended loss (7705 SAR only)
- CFM two-way SLM

A CFM continuity check test is automatically generated when you create an MD. When you execute the test and a connectivity fault is present, the MEP that detects the fault raises an alarm. See Chapter 32 for information about a specific Ethernet CFM diagnostic test.

MEPs

MEPs are configured at the edge of an MD and perform the following functions:

- periodically send CFM continuity check messages
- validate CFM PDU replies

- discard CFM PDU messages that are not in the MEP configuration
- initiate and respond to CFM test messages

MEPs can be added to services automatically or manually. When a MEP is assigned to a service manually, it associates its MEG with a single site on the service. When a MEP is assigned to a service automatically, it associates its MEG with all sites on the service. MEPs which are generated automatically can inherit test generation options from the SAP or Service Site. See Procedure 78-1 for more information.

You can also add MEPs to services during Ethernet CFM test configuration from the Service Topology map. See "Working with Ethernet CFM objects" in chapter 6 for more information.

Each MEP is assigned an up or down direction. An up MEP is provisioned on an ingress port, and monitors the forwarding path inside a bridge NE to the egress port. A down MEP is provisioned on an egress port, and monitors the forwarding path between bridge NEs.

You can configure an initial MEP ID for automatic MEP ID assignment on an NE. See Procedure 78-2 for more information.

You can assign roles to managed MEPs and unmanaged remote MEPs during OAM test suite configuration. A MEP can be designated as a hub or spoke, and as a test source, a test target, or both. Assigning roles to MEPs in test suites can reduce the total number of automatic tests generated. See Procedure 78-1.

MEPs can inherit their roles from the SAP or Service Site. You can propagate test generation role settings to all unmanaged remote and managed MEPs on a SAP or service site using the Propagate to MEPs button on the ETH-CFM tab of the Access Interface (Edit) and Site (Edit) forms.

An up MEP can be associated with the following object types:

- Epipe and VPLS SAPs
- Epipe spoke SDP bindings
- VPLS mesh and spoke SDP bindings
- VPLS and MVPLS B-sites, as virtual MEPs
- B-L2 access interfaces
- OmniSwitch VLAN SAPs

A down MEP can be associated with the following object types:

- Epipe, Ipipe, IES, VPLS, and VPRN SAPs
- Epipe and IES spoke SDP bindings
- VPLS mesh and spoke SDP bindings
- B-L2 access interfaces
- MVPLS access interfaces
- OmniSwitch VLAN SAPs
- Network interfaces
- Ports
- LAGs

Virtual MEPs

A virtual MEP is an up MEP that is created on a VPLS site when a CFM continuity check test is run. Each virtual MEP transmits a CFM continuity check stream on all SAPs and SDPs of the site. A virtual MEP uses the site MAC address, if configured; otherwise, it uses the shelf MAC address. See chapter 68 for information about assigning virtual MEPs to a VPLS.

The following rules apply to virtual MEP management:

- One virtual MEP can be configured on a VPLS or MVPLS B-site.
- All regular MEPs on SAPs and SDP bindings in the same MEG as a virtual MEP must be configured as up MEPs.
- Regular MEPs in the same MEG and on the same B-site as a virtual MEP cannot be enabled when the virtual MEP is enabled.
- Virtual MEPs can be created in a MEG only when MIP creation in the MEG is disabled.

Facility MEP

A facility MEP is a MEP that is down and is created on a router interface, network interface, port, or LAG. A facility MEP detects failure conditions for an Ethernet transport network using ETH-CCM or AIS and, where appropriate, propagates alarm conditions so that the services that share this common transport are aware of the failure.

A virtual tunnel facility MEP is created by configuring a LAG MEP or a port MEP with a VLAN ID. In this instance the VLAN ID must match the outer encapsulation value of the SAP that is associated with the Tunnel MEP.

The following rules apply to facility MEP management:

- Only one facility MEP can be configured on a port, a LAG, or a network interface.
- A facility MEP can be configured on a port only if the MD level is 0.
- A facility MEP must be configured in the down direction.
- A facility MEP ID must be unique within the same device.
- Port facility MEPs are supported on ports in access, hybrid, or network mode with dot1q encapsulation, and on ports in access or hybrid mode with Q in Q encapsulation.
- Port facility MEPs cannot be configured on network elements that support Ethernet tunnels.
- Tunnel facility MEPs are supported on LAG ports configured with Q in Q encapsulation in access or hybrid mode.
- Tunnel facility MEPs must have a lower MD level than any service MEPs that are created on the same LAG.
- A tunnel facility MEP VLAN ID must be unique within the same port.
- Tunnel facility MEPs cannot be configured on LAGs with a VLAN ID of 0.
- Tunnel port facility MEPs cannot be configured on LAG members.
- Fast facility MEPs, which are MEPs with a CCM interval of 10 ms or 100 ms, cannot be configured when CCM padding is enabled.
- There must be 2 facility MEPs in a MEG subgroup to execute a CCM test.

MIPs

Maintenance intermediate points, or MIPs, are internal points in an MD that perform the following functions:

- validate received CFM PDUs
- validate and respond to link trace messages
- validate and respond to loopback messages

A MIP consists of two half-function objects that allow the MIP to be recognized as a MIP in one MD level and as a MEP on a higher level.

Ethernet-CFM redundancy

When you configure Ethernet-CFM redundancy, you can link MEPs to the state of the resiliency mechanism that is supported in MC-LAGs. The state of the MEP does not affect the state of resiliency mechanism.

Ethernet-CFM redundancy is configured at the NE level. When you configure Ethernet-CFM redundancy, the state of a MEP is the same as the state of the SAP, LAG, or MC-LAG with which it is associated. For example, if the redundant MC-LAG is in standby state, the MEP is also in standby state. When a MEP is in standby state, the MEP is idle, CCMs are not exchanged, and the MEP does not respond to CFM tests.



Note — The MEP, SAP, and LAG must reside within an MC-LAG that has Ethernet-CFM redundancy configured. See Procedure 39-1 to configure MC-LAGs.

When Ethernet-CFM redundancy is configured and the active state of an MC-LAG changes, the MC-LAG Inactive state on the MEP changes and any defects on the MEP are flagged.

The state of MEPs, SAPs, and LAGs that are configured for Ethernet-CFM redundancy appears in the MC-LAG Inactive field. The status of MC-LAGs that are configured for Ethernet-CFM redundancy appears in the Is Active field.

In addition to configuring Ethernet-CFM redundancy at the NE level, you can configure Ethernet-CFM redundancy on tunnel MEPs. See Procedure 13-2 to configure Ethernet-CFM redundancy at the NE level. See Procedure 14-11 to configure Ethernet-CFM redundancy on a tunnel MEP.

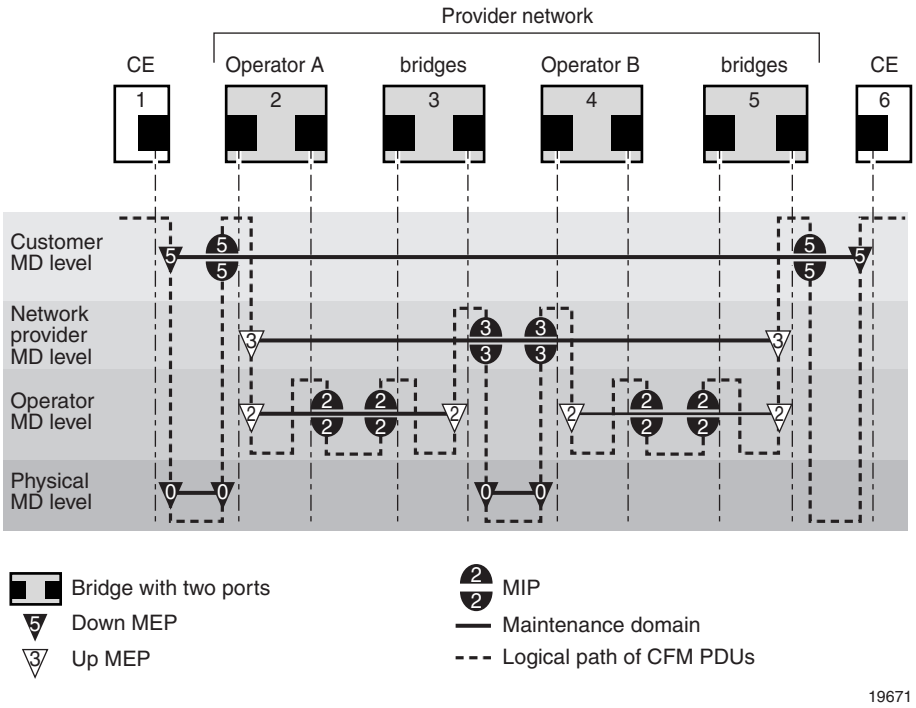
Sample Ethernet CFM implementation

Figure 78-1 shows an example of MDs, MEPs, and MIPs in a IEEE 802.1ag network that consists of two operator areas, for example, services in the provider network, that are joined to create a network path for customer traffic. The number on an object identifies the associated MD, which is one of the following:

- MD 5—end-to-end customer path
- MD 3—end-to-end network provider path
- MD 2—paths within services
- MD 0—physical path

MD 5 provides access to a down MEP on each CE device, and to a MIP on each PE bridge. MD 3 provides access to an up MEP on each PE bridge, and to a MIP on each bridge between groups of operator bridges. MD 2 provides access to the up MEPs and MIPs in each service. MD 0 provides access to MEPs for checking the physical connectivity between NEs.

Figure 78-1 Ethernet CFM objects in example network



Ethernet CFM implementation for composite services

End-to-end test suite generation for composite services is available for VPLS and VLL Epipe services. In this context, a composite service is a set of services connected by one or more of the following:

- VLAN uplinks
- Spoke bindings
- CCAG connectors

Creating test suites and test policies for composite services is very similar to creating these for a regular service. Test generation options can be applied to modify the roles of managed and remote unmanaged up MEPs. See Procedure 78-1. The Accounting Files and Continuously Executed options are also available when you create a test policy for a composite service.

Once tests have been ordered to generate, a MEG is created on each eligible endpoint SAP. Tests are then generated for this MEG that target other eligible endpoint SAPs within the composite service. Results for individual tests can then be reviewed.

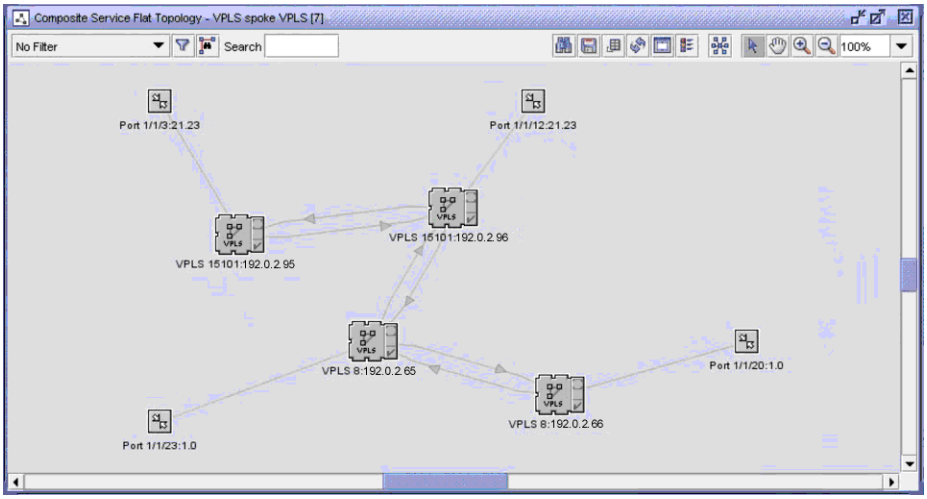
Note — If there is a previously created MEG on one of the service sites (for example, a MEG created for a service before the service was included in a composite service) and the Generate Tests button is selected, tests are not generated. When a MEG with only a subset of the composite service already exists on one of the service SAPs, the generation of tests is blocked. The MEG must be deleted before the CFM tests are generated.

Examples of Ethernet CFM tests for composite services

The following are examples of how the Ethernet CFM test generation rules for composite services are structured to operate.The examples are based on the default test roles for MEPs. The default roles are Hub and both Test Source and Test Target.

Figure 78-2 shows a flat topology view of a simple configuration of two VPLSs (VPLS 8 and VPLS 15101) that are connected by a pair of spoke bindings between sites 192.0.2.96 and 192.0.2.65.

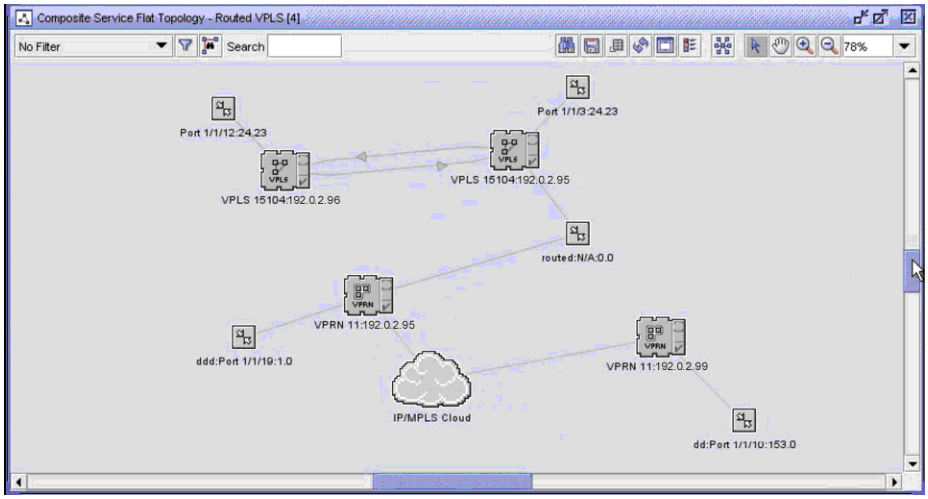
Figure 78-2 Composite service connected by spoke bindings



In this configuration, all four SAPs are considered as endpoints. Therefore MEPs are generated on each SAP and they all target each other. A total of twelve tests are generated. Double-clicking on an endpoint opens the interface configuration form and the MEP generated for this particular endpoint is displayed under the MEPs tab. If you then query the MEP's properties, the Tests tab in the MEP's configuration form displays the three tests that target the other MEPs in this composite service.

Figure 78-3 shows an example of a routed VPLS configuration with a VPLS (VPLS 15104) and a VPRN (VPRN 11). The services are connected by a routed VPLS interface (shown as routed:N/A:0.0).

Figure 78-3 Routed VPLS composite service



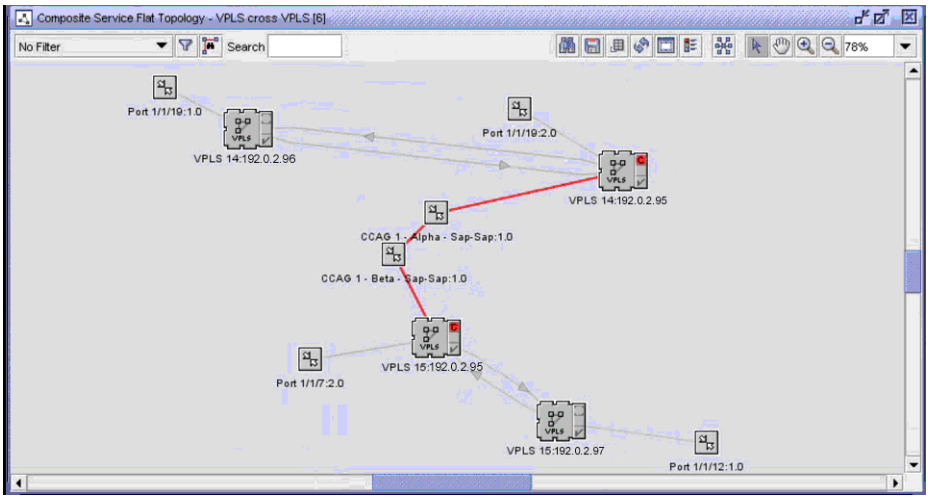
In this configuration, site 192.0.2.95 exists on both the VPLS and VPRN service. This is an overlapping site. The test generation rules would normally skip an overlapping site and no MEGs or tests would be generated for that site.

However in this case, the overlap for this site occurs in an unsupported service. The test generation rules for such a configuration will skip the unsupported VPRN service entirely and only generate tests for the supported VPLS, including site 192.0.2.95. Therefore, two MEPs and two tests (targeting each other) will be generated here, one for each of the SAPs on sites 192.0.2.96 and 192.0.2.95.

The test generation logs available in the test suite configuration form (under the Generation Logs tab) provide an explanation whenever the test generation rules cause items to be excluded from the tests. In this case, the log would state: “The CFM Composite Services Test Suite skipped the unsupported service”.

Figure 78-4 shows an example of a cross-connected VPLS composite service.

Figure 78-4 Cross-connected VPLS composite service



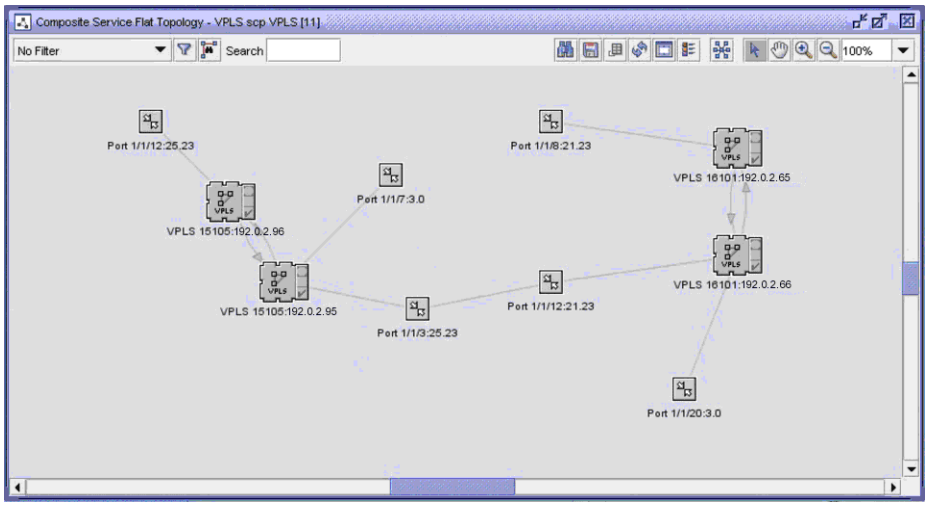
In this configuration, the two VPLSs (VPLS 14 and VPLS 15) are cross-connected by the SAPs CCAG 1-Alpha and CCAG 1-Beta. Both these SAPs originate from site 192.0.2.95, which exists in both services. It is therefore an overlapping site. The test generation rules skip overlapping sites, so no MEGs or tests are generated for any SAPs associated with that site.

Therefore, two MEPs and two tests (targeting each other) will be generated here, one for each of the SAPs on sites 192.0.2.96 and 192.0.2.97.

In addition, there will be two test generation logs available in the Generation Logs tab of the test suite configuration form. In this case, the logs would be identical, one stemming from each of the supported VPLSs. The logs would state: “Skipped overlapping service site”.

Figure 78-5 shows an example of an SCP-connected VPLS composite service.

Figure 78-5 SCP-connected VPLS composite service



In this configuration, the two VPLSs (VPLS 15105 and VPLS 16101) are joined by an SCP connector between sites 192.0.2.95 and 192.0.2.66. The test generation rules skip any SAPs identified as part of a connector, since they are not endpoints. So no MEGs or tests are generated for either connector SAP.

MEGs and tests will however, be generated for each of the other four SAPs shown in the example. In total, four MEGs and twelve tests will be generated.

In addition, there will be two test generation logs available in the Generation Logs tab of the test suite configuration form. In this case again, the logs would be identical, one stemming from each of the supported VPLSs. The logs would state: “Skipped service connecting SAPs”.

Primary VLAN support for Ethernet CFM

The Primary VLAN feature allows an operator to set a VLAN identifier to perform additional ETH-CFM extraction checking. Primary VLAN enabled MEPs will only perform the addition extraction routines for MEPs configured under the same SAP and that have an enabled Primary VLAN. When a MEP is configured without a Primary VLAN, only the classic extraction is performed.

By default, the ETH-CFM processing uses the exact SAP configuration to determine the proper offset for the start of the ETH-CFM e-type 0x8902 PDU. Any packet that includes ETH-CFM (e-type 0x8902) at the appropriate offset will be subjected to the extraction routines for MEPs or MIPs. If the ETH-CFM is not at the appropriate offset, the packets pass as user data.

The default mapping of the ingress packet to the SAP is based on the Layer 2 mapping. The mapping to the appropriate MEP is based on this Layer 2 look up. If there is not an exact match, as in the case of ambiguity or additional VLAN tags beyond the SAP delineation, then additional look ups for ETH-CFM are possible. This is mostly applicable to ambiguous SAPs, where a single VLAN or aggregate is transporting many VLANs underneath that aggregate function. It is also applicable to dot1q networks that carry multiple tags without using the default SAP. Fully-qualified SAPs are also able to use the Primary VLAN function. The extraction function is the same for either fully-qualified or ambiguous SAPs.

A MEP or MIP must be configured on a particular SAP to perform any ETH-CFM extraction. The classic extraction (which is the matching of the ETH-CFM packets immediately following the SAP configuration) is performed first. If the Ethernet encapsulation is set to dot1q and the SAP configuration is x/y/z:*, then the ETH-CFM extraction looks for ETH-CFM to appear in the header with no VLAN tags preceding it. If there is a match on this classic extraction, then there no further extraction routines are invoked. If the classic extraction fails and a second MEP is configured with Primary VLAN enabled, then the additional extraction will check to see if ETH-CFM immediately follows the specified Primary VLAN. If that is true, then the VLAN will be used as an index into the primary VLAN table and the extraction is performed based on normal criteria following the ETH-CFM rules.

The Primary VLAN function is supported for Up and Down MEPs, as well as Ingress and egress MIPs on an Ethernet SAP for VPLS and Epipe service MEPs (including Local Switched PBB ePipe with PBB Tunnel backup). Primary VLAN support is only applicable to service MEPs and not facility MEPs (specifically, not Tunnel MEPs). Facility MEPs are meant to validate the transport and not switching capability of a network element.

When enabling this function, an operator can specify the VLAN ID for generated MEG sites, and also whether or not the MEP should be a Primary VLAN MEP or MIP (only applicable to SAP MEPs or MIPs on VPLS and Epipe services)

The CCM test execution routine checks if all MEPs in the MEG or MEG Sub-group match before allowing the test execution to proceed.

Points to consider when enabling the Primary VLAN function:

- Alcatel-Lucent recommends that a unique MA should be employed for each Primary VLAN.
- The Primary VLAN function is only applied to SAPs (Virtual MEPs are not supported).
- The MHF-Creation parameter must be set to the static option to force the generation of Primary VLAN MIPs. This is suppressed on older or non-SR NEs.
- Primary VLAN MEPs can only be assigned at creation time.
- Primary VLAN MEPs must have an MA Service VLAN ID correctly set.
- The MA Service VLAN ID cannot be changed if Primary VLAN MEPs exist.

- Multiple Primary VLAN MEPs per SAP are supported. There is no restriction on the number of MEPs that are allowed on any SAP when employing this feature. Both the classic extraction context and every Primary VLAN on the SAP can support up to 16 MEPs (8 Up and 8 Down), one per MD level.
- All eight MD levels can be configure on all MEPs (0-7) that are configured on a SAP, within their specific context (classic or Primary VLAN). This allows an operator to have the complete range of eight MD levels for use in the specified primary VLAN. This avoids conflicts when the same MD Level and Layer 2 encapsulation maps to two different MEPs in the different contexts.
- Levels are specific within each of the contexts (classic and all the Primary VLANs configured on the same SAP). Therefore each lookup can have overlapping levels. The hierarchy is maintained within the extraction context.
- Primary VLAN MEPs and Fault Propagation are mutually exclusive.
- Primary VLAN MEPs and Fast CCM Interval are mutually exclusive.
- There is no sub second CCM support for Primary VLAN enabled MEPs.
- The Primary VLAN function is not applicable to Omni switches.

78.2 Workflow to configure Ethernet CFM

This workflow describes the procedures to create and run an Ethernet CFM test.

Ethernet CFM tests are configured through the 5620 SAM Service Test Manager. See chapter 77 for more information.

1 Configure the initial MEP ID value on an NE for automatic MEP creation. See Procedure 78-2 for more information.

2 Create an Ethernet CFM MD and subordinate objects associated with the MD such as a Global MEG, MEG, and MEP for each level at which Ethernet connectivity is to be monitored. See Procedure 78-1 for more information.

   i Create one or more global MEGs in each MD. Each MEG must be associated with one service or Ethernet path. Creating a Global MEG generates a CFM continuity check test.

   ii Associate a service with the Global MEG.

   iii As required, add an Ethernet path to the Global MEG.

   iv As required, add a managed MEP to the MEG.

   v As required, add a remote MEP to the MEG.

   vi As required, add an unmanaged remote MEP to the Global MEG.

   vii As required, add a MEG sub-group to a Global MEG.

3 As required, change the MEG sub-group association for managed MEPs or unmanaged remote MEPs. See Procedure 78-4 for more information.

4 As required, configure a default NE-level MD on an OmniSwitch. See Procedure 78-5 for more information.

5 Create a test policy, specifying at least one of the following Ethernet CFM test definitions:

- CFM Loopback
- CFM Link Trace
- CFM Two Way Delay Test
- CFM Two Way SLM

See Procedure 77-1 for more information.

6 Create a test suite. See Procedure 77-4 for more information.

7 As required, execute the generated Ethernet CFM test suite. See Procedures 77-6 and 77-8 for more information.

8 As required, view the test results. See Procedures 77-11, 77-12, and 77-13 for more information.

78.3 Ethernet CFM procedures

The following procedures describe how to configure and manage Ethernet CFM.

Procedure 78-1 To configure an Ethernet CFM MD and subordinate objects associated with the MD

Perform this procedure to configure an Ethernet CFM MD and subordinate objects associated with the MD such as a Global MEG, MEG, and MEP.

Many of the forms accessed in this procedure can also be accessed using the Service Topology map. See section 6.3 for information about working with maps.



Note — You can only perform this procedure when a service exists to associate with the MD or subordinate objects.

1 Choose Tools→Ethernet CFM→Maintenance Domain Policies from the 5620 SAM main menu. The Maintenance Domain Policies form opens.

2 Perform one of the following:

a Modify an existing MD.

i Configure a filter if required and click on the Search button. A list of MDs appears.

ii Select an MD in the list and click on the Properties button. The Maintenance Domain - Global Policy (Edit) form opens.

b Create a new MD.

i Click on the Create button. The Maintenance Domain - Global Policy (Create) form opens.

ii Configure the parameters:

- MD Mgr Object ID
- Maintenance Domain ID
- Auto-Assign ID
- Name Type
- Name
- Level

If the MD is to be used for Y.1731 performance measurement tests, you must set the Name Type parameter to none.

iii Click on the Apply button. The form displays additional tabs, and the form name changes to Maintenance Domain Global Policy (Edit).

iv Click on the Switch Mode button. A dialog box appears.

v Click on the Yes button. The Configuration Mode changes to Released.

3 Configure the Description parameter and click on the OK button. A dialog box appears.

4 Click on the Yes button. The Maintenance Domain - Global Policy (Edit) form closes, and the Maintenance Domain Policies form reappears.

5 Add a Global MEG to an MD.

i Select an MD in the list and click on the Properties button. The Maintenance Domain - Global Policy (Edit) form opens.

ii Click on the Global Maintenance Entity Group tab.

iii Click on the Create button. The Global Maintenance Entity Group (Create) form opens with the General tab displayed.

iv Configure the parameters:

- Auto-Assign ID
- Name
- Description
- Administrative State

v Configure the Name Format and Name parameters in the Maintenance Entity Group panel.

If you select icc-based as the Name Format, then the associated Name value must be 8 to 13 characters long.

vi Configure the parameters in the Initial MEG Configuration panel:

- Initial CCM Interval
- Initial MHF-Creation
- Initial CFM Hold Down Timer (Centiseconds)
- Initial MIP LTR Priority

When you are creating a Global MEG for a 7750 SR-c4, 7750 SR-c12, or 7450 ESS-6, the Initial CCM Interval must be set to 1s.

You can only configure the Initial CFM Hold Down Timer (Centiseconds) parameter when the Initial CCM Interval is set to10 ms or 100 ms.

When the Initial CCM Interval parameter is set to 10 ms or 100 ms, you cannot configure automatic MEP creation in step 7.



Note — When a Global MEG is created and applied, you can open the Global Maintenance Entity Group form at any time and view on the General tab two information fields that display the number of local MEGs and the number of MEPs currently associated with the Global MEG.

vii Click on the OK button. The Global Maintenance Entity Group (Create) form closes, and the Maintenance Domain - Global Policy (Edit) form reappears with the Global Maintenance Entity Group tab displayed. The Global MEG is listed on the form and a default MEG sub-group is added to the Global MEG.

6 To add a MEG sub-group to a Global MEG, perform one of the following, if required:

a Add a new MEG sub-group to a Global MEG.

i Select a Global MEG in the list and click on the Properties button. The Global Maintenance Entity Group (Edit) form opens with the General tab displayed.

ii Click on the MEG Sub-Group tab.

iii Click on the Create button. The MEG Sub-Group (Create) form opens.

iv Configure the parameters:

- MEG Sub-Group ID
- Auto-Assign ID
- Name
- Ignore test generation and CCM test

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The MEG sub-group is listed on the Global Maintenance Entity Group (Edit) form.

vii Click on the OK button to close the Global Maintenance Entity Group (Edit) form. A dialog box appears.

viii Click on the Yes button. The Global Maintenance Entity Group (Edit) form closes and the Maintenance Domain (Edit) form appears.

ix Close the Maintenance Domain (Edit) form. The Maintenance Domain Policies form appears.

b Automatically create a new MEG sub-group based on existing remote MEP lists.



Note — You can only create MEG sub-groups using this method when a valid remote MEP list exists and the remote MEPs on the list are CCM enabled.

i Select a Global MEG in the list and click on the Properties button. The Global Maintenance Entity Group (Edit) form opens with the General tab displayed.

ii Click on the Discover MEG Sub Groups button. If this button is not visible, click on the More Actions button and choose Discover MEG Sub Groups. When remote MEPs on valid lists are CCM enabled, new MEG sub-groups are created from the remote MEP lists. The new MEG sub-groups are listed on the Global Maintenance Entity Group (Edit) form.

iii Click on the OK button to close the Global Maintenance Entity Group (Edit) form. A dialog box appears.

iv Click on the Yes button. The Global Maintenance Entity Group (Edit) form closes and the Maintenance Domain (Edit) form appears.

v Close the Maintenance Domain (Edit) form. The Maintenance Domain Policies form appears.

7 To associate a service with a Global MEG, perform one of the following, if required:

a Automatically associate all NEs in a service with a Global MEG.

i Select an MD in the list and click on the Properties button. The Maintenance Domain - Global Policy (Edit) form opens.

ii Click on the Global Maintenance Entity Group tab.

iii Click on the Create button. The Global Maintenance Entity Group (Create) form opens with the General tab displayed.

iv Click on the Service tab.

v Click on the Create button. The Service (Create) form opens.

vi Click on the Select button. The Select Service form opens.

vii Click on the Search button. A list of services is displayed.

viii Select a service in the list and click on the OK button. The Select Service form closes, and the service information is displayed on the Service (Create) form.

ix Configure the Auto-Assign ID parameter.

x Configure the Follow Service Topology Changes parameter, if required.



Note — Enabling this parameter will cause relevant Ethernet OAM objects in the MEG and MEG sub-groups to automatically change in response to topology changes in the service or composite service you selected in step viii. Such changes include the addition or deletion of sites, SDP bindings, and access interfaces. Applicable CFM tests (as specified in a test suite) will then also be automatically generated and/or deleted, as required. The specific Ethernet OAM objects that will respond to a service topology change are dependent on the selections you make in step xii below.

xi Configure the parameters in the Auto-Creation of MEG(s) panel, as required:

- Auto MEG Site Creation
- VLAN ID
- Multi-Service MEG

xii Configure the parameters in the Auto-Creation of MEP(s) panel, as required:

- MEP(s) Creation on Access Interfaces
- Direction
- Primary VLAN Enable
- MEP(s) Creation on SDP Bindings
- Direction
- Virtual MEP(s) Creation on VPLS Sites
- Direction



Note — You cannot configure the MEP(s) Creation on Access Interfaces, MEP(s) Creation on SDP Bindings, or Virtual MEP(s) Creation on VPLS Sites parameters when the Initial CCM Interval parameter is set to 10 ms or 100 ms.

xiii Configure the parameters in the Auto-Creation of MIP(s) panel, as required:

- MIP(s) Creation on Access Interfaces
- Primary VLAN Enable
- MIP(s) Creation on SDP Bindings

xiv Click on the OK button. A dialog box appears.

xv Click on the OK button. The Service (Create) form closes, and the Global Maintenance Entity Group (Create) form reappears, with the service listed on the form.

b Associate a single NE on a service with a Global MEG.

i Select an MD from the list and click on the Properties button. The Maintenance Domain Global Policy (Edit) form opens.

ii Click on the Global Maintenance Entity Group tab and click on the Search button. A list of Global MEGs appears.

iii Select a Global MEG from the list and click on the Properties button. The Global Maintenance Entity Group (Edit) form opens.

iv Click on the NE Maintenance Entity Group tab.

v Click on the Create button. The NE Maintenance Entity Group (Create) form opens with the General tab displayed.

vi Click on the Select button in the Site panel. The Select Site form opens.

vii Click on the Search button. A list of sites is displayed.

viii Select a site in the list and click on the OK button. The Select Site form closes, and the site information is displayed on the NE Maintenance Entity Group (Create) form.

ix Configure the parameters:

- CCM interval
- VLAN ID
- MHF-Creation
- CFM Hold Down Timer (Centiseconds)

You can only configure the CFM Hold Down Timer (Centiseconds) parameter when the CCM interval is set to10 ms or 100 ms.

You cannot choose the 10 ms and 100 ms options for the CCM interval parameter when the CCM Padding Packet Size(Bytes) parameter is enabled.



Note — Only the parameters that are supported on the selected site are displayed when you open the form.

x Click on the Service tab of the NE Maintenance Entity Group (Create) form and then click on the Create button. The MEG Service (Create) form opens.

xi Configure the parameters:

- Service ID
- MHF-Creation
- VLAN ID
- Id-Permission
- MIP LTR Priority



Note — Only the parameters that are supported on the selected site are displayed when you open the form.

xii Click on the OK button. The MEG Service (Create) form closes, and a dialog box appears.

xiii Click on the OK button. The NE Maintenance Entity Group (Create) form displays, with the service listed on the Service tab.

xiv Click on the OK button. The NE Maintenance Entity Group (Create) form closes.



Note — When an NE Maintenance Entity Group is created and applied, you can open the NE Maintenance Entity Group (Edit) form at any time and view on the General tab an information field that displays the number of MEPs currently associated with the NE Maintenance Entity Group.

8 Add an Ethernet path to the Global MEG, if required.

i Click on the Ethernet Path tab.

ii Click on the Create button. The Ethernet Path (Create) form opens.



Note — You must specify an Ethernet tunnel path or Ethernet ring path on this form.

iii To add an Ethernet tunnel path, click on the Select button in the Ethernet Tunnel Path panel. The Select Ethernet Tunnel Path form opens. Otherwise, go to step vi.

iv Select an Ethernet tunnel path in the list and click on the OK button. The Select Ethernet Tunnel Path form closes, and the Ethernet tunnel path is displayed on the Ethernet Path (Create) form.

v Go to step viii.

vi Click on the Select button in the Ethernet Ring Path panel. The Select Ethernet Ring Path form opens.

vii Select an Ethernet ring path in the list and click on the OK button. The Select Ethernet Ring Path form closes, and the Ethernet ring path is displayed on the Ethernet Path (Create) form.

viii Configure the parameters:

- Auto-Assign ID
- Object ID
- Run Continuity Check Protocol
- Set Control MEP property on created MEPs

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Ethernet path is displayed on the Global Maintenance Entity Group (Create) form.

9 Perform the following steps to add an NE MEG to the MD, if required.

i Click on the NE Maintenance Entity Group tab.

ii Click on the Create button. The Maintenance Entity Group (Create) form opens with the General tab displayed.

iii Click on the Select button next to the System ID (Loopback IP Address) parameter. The Select Site form opens.

iv Click on the Search button. A list of sites is displayed.

v Select an NE in the list and click on the OK button. The Select Site form closes, and the Maintenance Entity Group (Create) form displays the NE information.

vi Click the Select button in the Unicast Hub MEP panel to configure the MEP ID parameter, if applicable and if required.



Note — The Unicast Hub MEP panel will only be displayed when the site you selected in step v is a 7450 ESS, 7750 SR, or 7950 XRS NE.

Configuring this parameter allows you to add a unicast MEP to the remote MEPs list. This enables the deployment of a hub-and-spoke topology where multiple MEPs acting as spokes can communicate with one hub MEP. So in this scenario, the remote MEP has a MEP Mac Address which is the Operational MAC Address of the Unicast Hub MEP.

Refer to the MEP ID parameter description for additional information and constraints on configuring a unicast CCM hub.

vii Configure the parameters, if applicable:

- CCM interval
- VLAN ID
- MHF-Creation
- CFM Hold Down Timer (Centiseconds)



Note 1 — The VLAN ID parameter is configurable only when the selected NE is an OmniSwitch.

Note 2 — The CFM Hold Down Timer (Centiseconds) parameter can only be configured when the CCM interval is set to 10 ms or 100 ms.

Note 3 — The 10 ms and 100 ms options of the CCM interval parameter cannot be configured when the CCM Padding Packet Size(Bytes) parameter is enabled.

viii To associate a template with the MEG, if required, click on the Templates tab. Otherwise, go to step xi.

ix Click on the Select button. The Select Associated Template - Maintenance Entity Group form opens.

x Select a template in the list and click on the OK button. The Select Associated Template - Maintenance Entity Group form closes, and the Maintenance Entity Group (Create) form displays the template information.

xi Click on the Service tab, if required. A list of services is displayed.

xii Click on the Create button. The MEG Service (Create) form opens.

xiii Configure the parameters:

- Service ID
- MHF-Creation
- VLAN ID
- Id-Permission

xiv Click on the OK button. The MEG Service (Create) form closes.

xv Click on the Apply button. A dialog box appears.

xvi Click on the OK button. The form name changes to Maintenance Entity Group (Edit), and the service is listed on the form, which displays additional tabs.

10 Perform the following steps to add a managed MEP to the MEG, if required.

i Click on the Managed MEP tab.

ii Click on the Create button. The MEP (Create) form opens.

iii Click on the Select button in the Maintenance Entity Group panel. The Select Maintenance Entity Group form opens.

iv Select a MEG in the list and click on the OK button. The Select Maintenance Entity Group form closes, and the MEG information is displayed on the MEP (Create) form.

v Configure the parameters:

- Direction
- Administrative State
- Description
- Mac Address
- Type
- Interface Type



Note 1 — The Interface Type parameter is configurable when the Type parameter is set to Regular.

Note 2 — The Interface Type Port is only available if the MD level is 0.

Note 3 — For facility MEPs, the Direction parameter must be set to Down.

vi Expand the CCM panel and configure the parameters as required:

- CCM Messages Enabled
- Fault Propagation
- CCM Padding Packet Size (bytes)
- Low-priority Defect
- Priority Level for CCM Messages

vii Click on the Select button in the MEG Sub-Grouping panel to associate the managed MEP to a MEG sub-group. The Select MEG Sub-Group form opens.

viii Click on the Search button. A list of MEG subgroups is displayed.

ix Choose a MEG subgroup and click on the OK button. The Select MEG Sub-Group form closes, and the MEG subgroup information is displayed on the MEP (Create) form.



Note — If a MEG subgroup is not selected, the managed MEP is automatically associated with the default MEG subgroup.

x Expand the Test Generation Options panel and configure the parameters as required:

- Role
- Use as Test Source
- Use as Test Target



Note 1 — The Role, Use as Test Source, and Use as Test Target parameters are configurable only when you set the Direction parameter to Up.

Note 2 — You can propagate test generation role settings to all MEPs on a SAP or service site using the Propagate to MEPs button on the ETH-CFM tab of the Access Interface (Edit) and Site (Edit) forms.

xi If the Type parameter you configured in step v is set to Virtual, go to step xviii.

xii If the Interface Type you configured in step v is set to LAG or Port, configure the Facility Fault Notify parameter.

xiii If the Interface Type you configured in step v is set to LAG, configure the Facility VLAN ID.



Note — If you are configuring a tunnel facility MEP, Facility VLAN ID must match the outer encapsulation value of the SAP to which you are connecting the tunnel facility MEP.

xiv Click on the Select button in the bottommost panel to choose an object of the type specified by the Interface Type parameter you configured in step v. The Select *object_type* form opens.

xv Click on the Search button. A list of objects is displayed.

xvi Select an object in the list and click on the OK button. The Select *object_type* form closes, and the object information is displayed on the MEP (Create) form.

xvii Go to step xxi.

xviii Click on the Select button in the Service Site panel to choose a site for the virtual MEP. The Select Service Site Pointer form opens.

xix Click on the Search button. A list of sites is displayed.

xx Select a site in the list and click on the OK button. The Select Service Site Pointer form closes, and the site information is displayed on the MEP (Create) form.

xxi If the MD for the MEP has a Name Type of none and its Maintenance Association has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable. Otherwise, go to step xxvi.

xxii Click on the Y.1731 TEST tab.

xxiii Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

xxiv Click on the AIS tab.

xxv Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

xxvi Click on the ETH-CSF tab.

xxvii Configure the parameters:

- Enable Client Signal Fault
- CSF Rx Multiplier

The CSF Rx Multiplier parameter is configurable when the Enable Client Signal Fault parameter is enabled.



Note 1 — ETH-CSF acts as one of the triggers for fault propagation on the receiving MEP, when the Fault Propagation parameter is enabled in step vi.

Note 2 — When the CSF Rx Multiplier is 0 (meaning that CSF will never timeout) and you need to manually clear the CSF state, you must first disable and then re-enable the Enable Client Signal Fault parameter. Otherwise, CSF must receive a C-DCI flag in a PDU to clear the state automatically, whenever the multiplier is 0.

Note 3 — If the CSF Rx Frame State read-only indicator displays anything other Client Defect Clear Indication, then a fault exists.

xxviiiClick on the OK button. A dialog box appears.

xxix Click on the OK button. The MEP is listed on the Global MEG (Create) form.

11 Perform the following steps to add a remote MEP to the MEG, if required.



Note 1 — You can add only one entry to the remote MEP list for a 7705 SAR.

Note 2 — When you execute a CCM test or synchronize the managed and unmanaged remote MEP lists, the 5620 SAM automatically distributes the local MEP and the remote MEP to the remote MEP list, except for 7705 SAR NEs, which are excluded from automatic MEP -distribution.

Note 3 — When you execute a CCM test or synchronize the managed and unmanaged remote MEP lists within a MEG sub-group, the 5620 SAM automatically distributes the local MEP and the remote MEP within that MEG sub-group.

Note 4 — If the remote MEP you are adding is to act as a Unicast Hub MEP, the remote MEP's MEP Mac Address will become the Operational MAC Address of the Unicast Hub MEP. If you subsequently delete the remote MEP, the Operational MAC Address of the configured Unicast Hub MEP will also be cleared.

Note 5 — If a local MEP and the corresponding remote MEP are on the same OmniSwitch, deleting the remote MEP results also deletes the corresponding local MEP.

i Click on the Remote MEP tab. The Remote MEP (Create) form opens.

ii Configure the MEP ID and MEP Mac Address parameters.

Refer to the MEP ID parameter description for additional information and constraints when configuring a remote MEP to act as a unicast CCM hub.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The remote MEP is listed on the Maintenance Entity Group (Edit) form.

12 Click on the OK button. The Maintenance Entity Group (Edit) form closes, and the MEG is listed on the Global Maintenance Entity Group (Edit) form.

13 Perform the following steps to add an unmanaged remote MEP to the Global MEG, if required.

i Click on the Unmanaged Remote MEP tab.

ii Click on the Create button. The Unmanaged Remote MEP (Create) form opens.

iii Configure the parameters:

- MEP ID
- MEP Mac Address

iv Click on the Select button in the MEG Sub-Group panel to associate the unmanaged remote MEP to a MEG sub-group. The Select MEG Sub-Group form opens.

v Click on the Search button. A list of MEG subgroups is displayed.

vi Select a MEG sub-group in the list and click on the OK button. The Select MEG Sub-Group form closes, and the MEG sub-group information is displayed on the Unmanaged Remote MEP (Create) form.



Note 1 — If a MEG sub-group is not selected, the unmanaged remote MEP is automatically associated with the default MEG subgroup.

Note 2 — The outline color of a MEP icon indicates the MEG subgroup to which the MEP belongs.

vii If required, expand the Test Generation Options panel. Configure the parameters:

- Role
- Use as Test Source
- Use as Test Target



Note 1 — The Role, Use as Test Source, and Use as Test Target parameters are configurable only when you set the Direction parameter to Up.

Note 2 — You can only configure Test Generation Options when the unmanaged MEP has a MAC address.

Note 3 — You can propagate test generation role settings to all MEPs on a SAP or service site using the Propagate to MEPs button on the ETH-CFM tab of the Access Interface and Site (Edit) forms.

viii Click on the OK button. A dialog box appears.

ix Click on the OK button. The unmanaged remote MEP is listed on the Global Maintenance Entity Group (Edit) form.

14 Click on the Synchronize Remote MEPs button to distribute the MEPs to the NEs, if required.



Note — If the managed MEP or unmanaged remote MEP belongs to a MEG sub-group, the remote MEP synchronization will only occur within the MEG sub-group.

15 Click on the Resync Remote MEP DB button to re-synchronize the Remote MEPs database, if required.

Optionally, you can also view the DB state of any Remote MEP under a Managed MEP by performing the following sub-steps. Otherwise, go to step 16.

i Click on the Managed MEP tab in the Global MEG form and click the Search button.

ii Select the required Managed MEP and click the Properties button. The MEP (Edit) form opens.

iii Click the Remote MEP DB State tab and click the Search button. A list of Remote MEPs communicating with the Managed MEP appears.

iv Select the required Remote MEP from the list and click Properties. The Remote MEP DB State (View) form opens, with the General tab displayed.

The presented information includes:

- MEP ID
- Remote State
- Grace Period RX
- MAC Address
- Rdi
- Port Status
- Interface Status
- Last CCM

v Click Cancel to close the Remote MEP DB State (View) form.

16 Click the Audit Unicast CCM item in the More Actions button fly-out menu to have the 5620 SAM automatically populate all the Hub pointers, if required.



Note 1 — For discovered networks with CCM and a remote MEP list configured, Alcatel-Lucent highly recommends the use of this button to set up a correct HUB-spoke topology in 5620 SAM before executing a CCM test.

Note 2 — The Audit Unicast CCM action will use the remote lists from all NEs to automatically set the Hub MEP pointers to the appropriate MEPs. If an appropriate MEP is not found, an unmanaged MEP with MEP ID and MEP MAC Address matching the unicast remote MEP entry will be created. The Hub MEP pointer is then set to this unmanaged MEP.

If duplicate managed and unmanaged MEPs are detected, the unmanaged MEP will be deleted and the managed MEP will be used as the unicast Hub MEP. This action will also ensure that the Hub MEP is in the same sub-group as the spoke pointing to it.

17 Click on the OK button. A dialog box appears.

18 Click on the Yes button. The Global MEG (Create) form closes, and the Maintenance Domain (Edit) form reappears.

19 Close the Maintenance Domain (Edit) form.

20 Close the Manage Maintenance Domain Policies form.

Procedure 78-2 To configure automatic MEP ID assignment on an NE

Perform this procedure to configure an initial MEP ID value on an NE for automatic MEP creation.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure automatic MEP ID assignment and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Globals tab.

4 Click on the OAM sub-tab.

5 Configure the MEP ID parameter.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The NE properties form closes.

Procedure 78-3 To automatically create identical MEPs on a redundant pair of service SAPs

Perform this procedure to create identical MEPs on service SAPs that are part of an MC-LAG. The procedure assumes that the service has been configured with MC-LAGs and redundant SAPs. The pair of redundant SAPs must have identical inner and outer encapsulations configured and they must be in the same service.

Refer to Procedure 14-10 for information on creating LAGs and to Chapter 39 on creating MC-LAGs.

1 Select Manage→Service→Services. The Manage Services form opens.

2 Click on the Search button. A list of services is displayed.

3 Select the required service from the list and click on the Topology View button. The Service Topology map opens.

4 Select the OAM check box at the bottom left of the map window. MEG and MEP objects are added to the map.

5 Perform one of the following:

a If you are creating a Global MEG:

i Right-click on the topology map background and select Create CFM Global MEG from the contextual menu. The Global Maintenance Entity Group (Create) form is displayed. Refer to Procedure 78-1 for information on configuring a Global MEG.

ii Once the Global MEG is created, a purple triangular MEP icon appears above each of the SAPs. Right-click on one of the MEP icons associated with the redundant pair of SAPs. The MEP (Edit) form for that SAP is displayed.

iii Click on the Properties button in the Redundancy panel.

This action automatically populates the Properties page of the redundant partner, thereby creating identical MEPs on both members of the redundant pair. Leave the MEP (Edit) form open.

iv Right-click on the other MEP icon associated with the redundant pair of SAPs. The MEP (Edit) form for that SAP is displayed.

v Confirm that the ID and Operational Mac Address parameters in the Redundant MEP panel for both MEPs are identical.



Note — If the redundant SAPs are in a VPRN or IES service, only the ID parameter will be synchronized between the two SAPs. Mac Addresses are not supported for these services.

b If you are working with an existing Global MEG where a MEP is missing from one of the SAPs in a redundant pair:

i Right-click on the MEP icon that is present for a SAP in the redundant pair. The MEP (Edit) form for that SAP is displayed.

ii Enable the Create Redundant MEP check box in the Redundancy panel.

iii Click the Apply button. A new MEP icon appears above the other SAP of the redundant pair.

This action automatically populates the Properties page of the redundant partner which was missing its MEP, thereby creating identical MEPs on both members of the redundant pair. Leave the MEP (Edit) form open.

iv Right-click on the new MEP icon. The MEP (Edit) form for that SAP is displayed.

v Confirm that the ID and Operational Mac Address parameters in the Redundant MEP panel for both MEPs are identical.



Note — If the redundant SAPs are in a VPRN or IES service, only the ID parameter will be synchronized between the two SAPs. Mac Addresses are not supported for these services.

6 Click on the OK button in both MEP (Edit) forms to close them.

Procedure 78-4 To change the MEG sub-group association for managed MEPs or unmanaged remote MEPs

Perform this procedure to change the MEG sub-group association for managed MEPs or unmanaged remote MEPs.



Note — The outline color of a MEP icon indicates the MEG sub-group to which the MEP belongs.

1 Select Manage→Service→Services. The Manage Services form opens.

2 Click on the Search button. A list of services is displayed.

3 Select a service in the list and click on the Topology View button. The Service Topology map opens.

4 Select the OAM check box at the bottom left of the map window. MEG and MEP objects are added to the map.

5 Right-click the interface object that includes the MEP that you wish to move to another MEG sub-group and choose Ethernet CFM→Edit MEP from the contextual menu.The Select MEP (Edit) form opens.

6 In the MEG Sub-Group panel, click on the Clear button to remove the current MEG sub-group association.

7 Click on the Select button. The Select MEG Sub-Group form opens.

8 Click on the Search button. A list of MEG sub-groups is displayed.

9 Click on an MEG sub-group and click on the OK button. The Select MEG Sub-Group form closes and the MEG sub-group information is displayed in the MEG Sub-Group panel.

10 Click on the OK button. The MEP (Edit) form closes, the MEP object color changes, and the MEP is moved to the newly selected MEG Sub-Group.

Procedure 78-5 To configure a default MD on an OmniSwitch

Perform the following procedure to configure a default NE-level MD on an OmniSwitch.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the OmniSwitch NEs icon.

3 Right-click on the device where you want to configure a default MD and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 Click on the Globals tab.

5 Click on the CFM tab.

6 Configure the parameters:

- Level
- MHF-Creation
- Id-Permission

7 Close the Network Element (Edit) form.

79 — Tunnel administrative groups

79.1 Tunnel administrative groups overview *79-2*

79.2 Workflow to configure tunnel administrative groups *79-3*

79.3 Tunnel administrative group procedures *79-3*

79.1 Tunnel administrative groups overview

The 5620 SAM supports SDP admin groups—or steering parameters—on all NEs and on all service tunnel types, prior to release 11.0. However, steering parameters are a logical concept within the 5620 SAM, and are not deployed to NEs. In release 11.0 of the 7750 SR, the support of SDP admin groups is introduced on the NE. SDP admin groups enable services to use a PW template to automatically include or exclude specific provisioned SDPs.



Note — For more information about SDP admin groups on the 7750 SR, see the specific device documentation.

In the 5620 SAM, Release 11.0, steering parameters are renamed to tunnel administrative groups. Tunnel administrative groups include not only the concept of steering parameters, but also 7750 SR SDP admin groups.

Tunnel administrative groups use the 5620 SAM policy distribution model. You can create a global tunnel administrative group and distribute it locally to NEs. Consider the following when you create a tunnel administrative group:

- you can create a maximum of 32 tunnel administrative groups
- the group value is uniquely associated with the group name
- an SDP can be added to more than one tunnel administrative group
- tunnel administrative groups are supported on:
  - GRE service tunnels
  - MPLS:BGP service tunnels
  - MPLS:LDP service tunnels
  - RSVP-LSP service tunnels
  - mixed LSP mode service tunnels

SDPs that share a specific characteristic or attribute can be made members of the same tunnel administrative group. When you create a service PW template, you can include and exclude one or more tunnel administrative groups. When a service is bound to the template, the SDP selection rules enforce the specified tunnel administrative group inclusion and exclusion constraints. Tunnel administrative groups allow you to control the SDP, or set of SDPs, that are selected while spokes are established among service sites using PW templates in BGP-AD, BGP-VPLS, or MS-PW applications. Tunnel administrative groups can be assigned to services that use the PW template policy, such as BGP-AD VPLS services, BGP-VPLS services, and Epipe spoke SDP FEC services. See chapter 73 for more information about PW template policies.

In addition, you can apply tunnel administrative groups to tunnel selection profiles. Tunnel selection profiles assign transport tunnels for a service when the service has been configured for automatic SDP binding creation. When a tunnel selection profile is used within a service to create SDP bindings, any tunnels that include the tunnel administrative group in that profile become eligible for consideration in the tunnel selection process. See chapter 27 for more information about tunnel selection profiles.

79.2 Workflow to configure tunnel administrative groups

The following workflow describes the high-level tasks required to create and configure tunnel administrative groups.

1 Create a tunnel administrative group. See Procedure 79-1.

2 Release and distribute the tunnel administrative group to the NEs. See Procedure 79-1.

3 Assign the tunnel administrative group to one or more of the following:

- A service tunnel. See Procedure 27-1 in chapter 27.
- A tunnel selection profile. See Procedure 27-3 in chapter 27.
- A service PW template. Ensure that the Use Provisioned SDP parameter on the service PW template is enabled. See Procedure 73-1 in chapter 73.
- A BGP or BGP AD VPLS. See Procedure 68-57 in chapter 68.

79.3 Tunnel administrative group procedures

Use the following procedures to configure 5620 SAM tunnel administrative groups.

Procedure 79-1 To create a tunnel administrative group

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form opens.

2 Click on the Create→Tunnel Admin Group button. The Tunnel Admin Group, Global Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Name
- Value

4 Click on the Apply button. The Tunnel Admin Group, Global Policy (Edit) form refreshes with additional tabs.

5 Click on the Distribute button to manually distribute the tunnel administrative group locally to devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute.



Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution, which also distributes the policy to existing local definitions.

6 Close the Tunnel Admin Group, Global Policy (Edit) form.

7 Close the Manage Service Tunnels form.

Procedure 79-2 To list and view tunnel administrative groups

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form opens.

2 Choose Tunnel Admin Group (Service Tunnel Management) from the object drop-down list.

3 Click on the Search button. A list of tunnel administrative groups appears.

4 Choose a tunnel administrative group and click on the Properties button. The Tunnel Admin Group - Global Policy (Edit) form opens with the General tab displayed.

5 Click on the following tabs for additional information:

- Local Definitions
- Service Tunnels—lists the service tunnels to which this tunnel administrative group is assigned, based on ID only
- Tunnel Selection Profiles— lists the tunnel selection profiles that include or exclude this tunnel administrative group, based on ID only
- Service PW Templates— lists the service PW templates that include or exclude this tunnel administrative group, based on ID only
- Faults—lists the alarms raised for the policy

6 Close the Tunnel Admin Group, Global Policy (Edit) form.

7 Close the Manage Service Tunnels form.

80 — RCA audit

80.1 RCA audit overview *80-2*

80.2 Workflow to configure RCA audit *80-8*

80.3 RCA audit procedures *80-9*

80.1 RCA audit overview

The 5620 SAM RCA audit tool allows you to perform on-demand or scheduled verifications of the configuration of services and physical links to identify possible configuration problems. Except for physical links, the 5620 SAM provides a solution, which, at your request, can automatically be implemented to make all the required configuration changes.



Note — The adjustments are made only to the 5620 SAM database and are not deployed to the network.

You can perform RCA audits of the following objects:

- VLL services
- VPLS services
- VPRN services
- physical links
- OSPF interfaces, areas, and area sites (5620 SAM/5650 CPAM integration only)
- IS-IS interfaces and sites (5620 SAM/5650 CPAM integration only)
- 9471 WMM instances and golden configurations



Note 1 — You need the 5650 CPAM license to perform the OSPF and IS-IS RCA audits. See the *5650 CPAM User Guide* for more information.

Note 2 — See "9471 WMM golden configuration management" in the *5620 SAM LTE EPC User Guide* for information about performing golden configuration RCA audits on 9471 WMM instances.

5620 SAM service audit

A 5620 SAM service is defined as a collection of service sites with the same customer ID, service type, and service ID. The 5620 SAM discovers services that are configured on a 7210 SAS, 7450 ESS, 7710 SR, 7750 SR, or 7950 XRS, using the service ID on the NE. Configuration errors may occur in networks where the services were created and deployed on the NEs using CLI before the NEs were managed by the 5620 SAM.

For example, when two VPLSs with the same service ID and the same mesh VC ID on an NE are discovered by the 5620 SAM, they are discovered as a single service in the 5620 SAM.

Another example of a configuration error is when a switching Epipe has multiple Epipe sites and multiple VC IDs for different segments. If different service IDs are used when the sites are created, the 5620 SAM assumes that the sites are connected and creates multiple VLL services within a composite service.

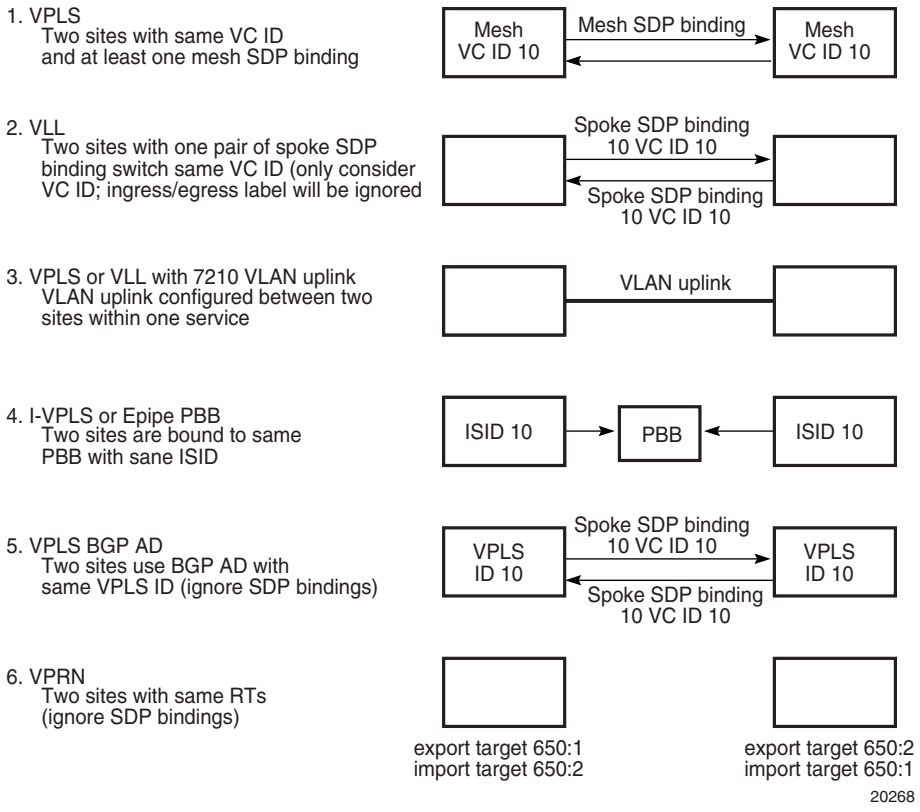
RCA audit policies allow you to modify the component membership of your 5620 SAM services to detect possible configuration problems. In addition, you can use the RCA audit to correct most configuration problems that are discovered in the audit.

Note — A 5620 SAM user who is assigned the Administrator or RCA scope of command role can create, modify, and execute all RCA audit policies. A 5620 SAM user who is assigned the Administrator or Service scope of command role can execute service audit adjustments.

Service membership rules

The 5620 SAM uses the rules in Figure 80-1 to identify whether two service sites are connected together. When two sites are identified as connected, they should belong to same service.

Figure 80-1 Rules to check whether two sites are connected



If service sites have different customer IDs, the 5620 SAM discovers the sites as belonging to different services. After the audit, the 5620 SAM generates a problem for each service. You can specify to which service the 5620 SAM should move the site and whether the empty service should be removed after the sites are moved.

For VPLS or VLL services, if the same service ID is used for two groups of sites that are not connected, the 5620 SAM detects a duplicate service ID. Two problems are generated for one of the group of sites, and the solution is to separate the services. If there are other groups of isolated sites, additional problems are generated for each group.

Consider the following when you perform an audit of a VPLS.

- Although different service IDs may be used, I-sites that are bound to same backbone VPLS and have the same ISID are considered to be in the same VPN.
- For VPLS sites that use BGP auto-discovery, the VPLS ID is used to determine service membership.
- H-VPLS is discovered as composite service in the 5620 SAM if different service IDs are used.

Consider the following when you perform an audit of a VLL service.

- Service sites with different customer IDs are discovered as two services, and can reconfigured as one service.
- More than two groups of sites that are connected can be detected and can be separated into different services.
- Redundant VLLs are not be affected by the audit and are considered correctly configured.
- If two Epipe sites are connected to the same PBB with same B-VPLS service ID, and the source and destination MAC addresses match, the 5620 SAM determines that the two sites are connected. If they are in different 5620 SAM services, a problem is generated during the audit.

Consider the following when you perform an audit of a VPRN service.

- VPRN service membership is based on the RTs defined in the VRFs.
- Sites that are in different services but have common import and export route targets. Import target of Site 1 is equal to the Export target of Site 2.

Physical link audits

Physical links represent the actual physical configuration of network connections between ports. You can view and manage physical links from the equipment window, physical topology map, and the Manage Equipment list form of the 5620 SAM, on each router using the CLI. Because several key parameters on each end of the physical link depend on each other, configuration errors are possible. The 5620 SAM RCA audit tool allows you to identify configuration errors in physical links. The 5620 SAM does not provide a solution for configuration problems that the RCA audit identifies for physical links. By default, the RCA audit detects the following configuration errors in physical links:

- **physical port parameters**
  - mismatched MTU values
  - mismatched speeds
- **Ethernet port parameters**
  - Auto-negotiate parameter misconfiguration
  - Duplex parameter misconfiguration

You can configure the RCA audit policy for the physical link to include additional physical link properties in the audit.

Viewing and analyzing RCA audit results

The RCA Audit Problem(s) indicator on the General tab of a network object properties form identifies whether configuration problems were detected in previous audits. The Last Audit Time indicator displays a timestamp of the last audit that was performed. The RCA Audit button is located at the bottom of the service properties form, or under the More Actions button.

After you associate an audit policy with the object, you can perform an RCA audit and view the results. If no problems are detected, the RCA Result tab does not appear.

The properties form of a problem displays the following information:

- problem severity
- probable cause
- description
- solution

The Caused By Objects tab lists the network objects that caused the problem. For service audits, the sites that should be moved out of a service, and the service they should move to, if there is only one destination service, are listed. If only one group of sites is listed, a new service is created and the sites are moved to the created service.

Table 80-1 describes the probable causes of problems.

Table 80-1 Probable causes

Probable cause	Description
Admin Down	The object is administratively down.
Aggregated	Aggregated cause
B-VPLS Backbone Attributes misconfigured	One or more B-VPLS backbone parameters are not configured correctly.
Control B-VPLS SPB ECT-FID mapping configurations are not consistent across all sites in this B-VPLS	The ECT algorithm to FID range mapping in a control SPB B-VPLS is not consistent on all of the sites in the same service. Each B-site must have the same number of ECT-to-FID mappings. In addition, the following ECT-to-FID range mapping parameters must be the same on all of the sites in the SPB-enabled B-VPLS: • FID Range Start • FID Range End • FID Range Algorithm See Procedure 68-61 for more information.
Misconfiguration	There is a misconfiguration error.
Missed service members for Multi-Segment PW	Missed service members for Multi-Segment PW

(1 of 3)

Probable cause	Description
No members configured for this Multi-homing site	The BGP VPLS multi-homing site does not have other sites as members that share the same multi-homing ID in order to comprise a group.
No valid Route Targets configured for VPLS BGP Multi-homing	No valid Route Targets currently exist for a VPLS site that has BGP multi-homing sites configured under it.
One or more SPB SAP(s) or SPB Spoke SDP Binding(s) exist on User B-VPLS that do not exist on Control B-VPLS. These extra links are not fate shared with the Control B-VPLS	One or more SPB SAPs or spoke SDP bindings on the user B-VPLS are not on the control B-VPLS. You must remove the SAPs or spoke SDP bindings, or create them on the control SPB B-VPLS site.
Route Targets are misconfigured for VPLS BGP Multi-homing	One of the following misconfigurations exists: • No matching RT for peered multi-homing sites • There are multiple RTs configured for a VPLS site that has BGP multi-homing sites configured under it. Multiple RTs will make the BGP multi-homing sites appear under multiple topologies or multiple services. • Multi-homing sites have the same multi-homing ID but different RTs (different RTs mean the sites are in different topologies or services)
Service Membership Misconfigured	The service membership is not configured correctly.
One or more SPB SAP(s) or SPB Spoke SDP Binding(s) configured on Control B-VPLS are missing from the User B-VPLS	One or more SPB SAPs or spoke SDP bindings are configured on the control B-VPLS that do not exist on this user B-VPLS. You must remove the SAPs or spoke SDP bindings, or create them on the user SPB B-VPLS site.
SPB is not enabled on one or more B-Sites in this B-VPLS	The SPB Mode parameter is not set to Control or User on one or more of the sites in the SPB-enabled B-VPLS service. See Procedures 68-61 and 68-62 for more information.
SPB Sites within this B-VPLS service do not have their SPB Modes (Control/User) consistently configured	One or more B-sites in the SPB-enabled B-VPLS service do not have the same value configured for their SPB Mode parameter as the other sites within the service. See Procedures 68-61 and 68-62 for more information.
The B-VPLS SPB FIDs are not identical across all sites in this B-VPLS service	The Forwarding Identifier (FID) parameter is not the same for all the sites in the SPB B-VPLS service. See Procedures 68-61 and 68-62 for more information.
The Control B-VPLS SPB unicast forwarding tree topology configurations are not consistent across all sites in this B-VPLS	The Unicast Forwarding Tree Topology parameter is not configured consistently on all of the sites in the same control SPB B-VPLS service. See Procedure 68-61 for more information.
Underlying Resource Operational Down	The underlying resource of the object is operationally down.
Underlying Resource Admin Down	The underlying resource of the object is administratively down.
Underlying Resource Missing	An underlying resource is missing.
Underlying Resource Problem	Problem with an underlying resource
Unknown	The probable cause could not be determined.

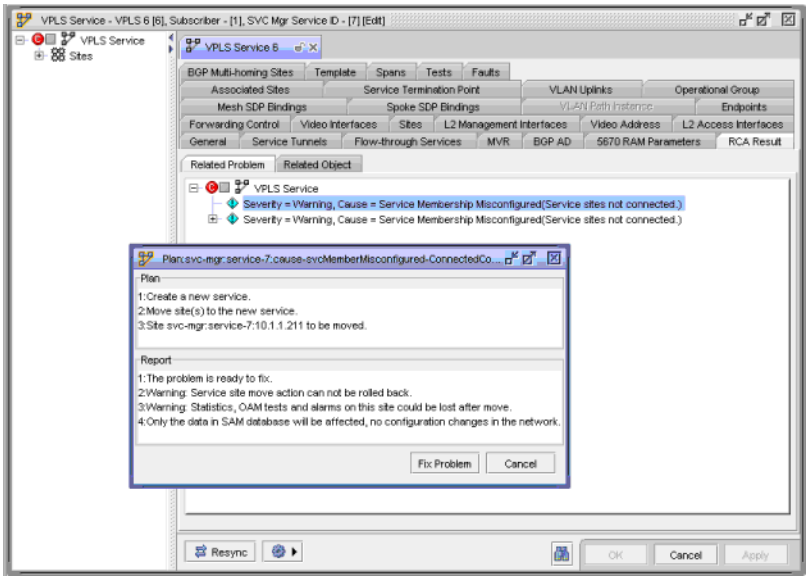
(2 of 3)

Probable cause	Description
Within this Control B-VPLS, not all SAPs or Spoke-SDPs are SPB enabled	SPB is not enabled on one or more SAPs or spoke SDP bindings in the control B-VPLS service. You must add the SPB interface to the SAP or spoke SDP binding. See Procedure 68-61 for more information.

(3 of 3)

You can use the RCA audit tool to correct a detected configuration problem from the RCA Result tab on the network object properties form. The 5620 SAM lists the operations to fix the problem, as shown in Figure 80-2.

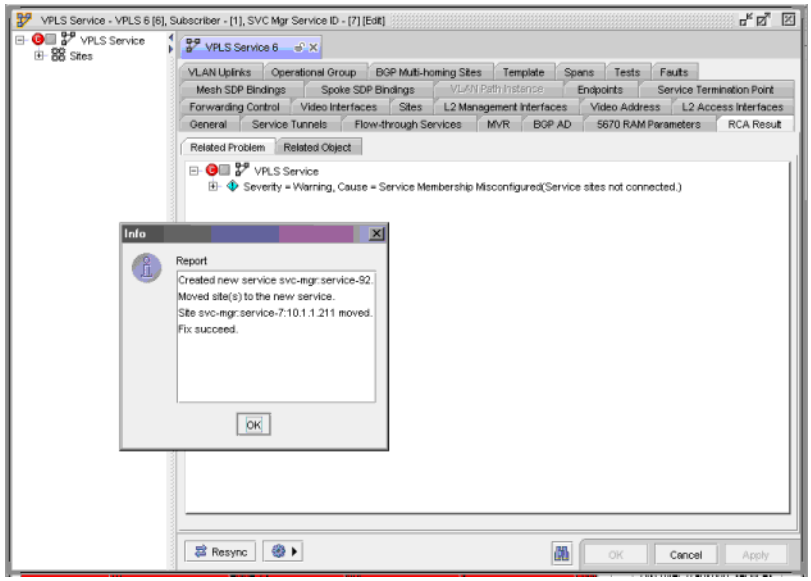
Figure 80-2 Correction plan for a problem



When you accept the proposed solution, a summary of the correction operation that the 5620 SAM implemented appears, as shown in Figure 80-3. To view the result in the server or client log, you must enable the logging option in the nms-server.xml or nms-client.xml file.

Caution — Contact your Alcatel-Lucent technical support representative before you attempt to modify the nms-server.xml file. Modifying the nms-server.xml file can have serious consequences that can include service disruption.

Figure 80-3 Correction report



80.2 Workflow to configure RCA audit

1. Create or configure an RCA audit policy. For service audits, configure one or more audit policies for each service type to detect different configuration problems. See Procedure 80-1 for more information.
2. Run the RCA audit policy for a specific service or object.
   - **a** Perform an RCA audit of a VLL service. See Procedure 80-2 for more information.
   - **b** Perform an RCA audit of a VPLS. See Procedure 80-3 for more information.
   - **c** Perform an RCA audit of a VPRN service. See Procedure 80-4 for more information.
   - **d** Perform an RCA audit of multiple services. See Procedure 80-5 for more information.
   - **e** Perform an RCA audit of a physical link. See Procedure 80-6 for more information.
3. Alternatively, create a service audit to run at a scheduled time. See Procedure 80-7 for more information.
4. Identify the problems and view the suggested solutions. Solutions are not provided for physical links.
5. Implement the changes, as required.

80.3 RCA audit procedures

Use the following procedures to perform RCA audit tasks.

Procedure 80-1 To configure an RCA audit policy

1 Choose Policies→RCA Audits from the 5620 SAM main menu. The RCA Audits form opens.

2 Select Audit Policy (RCA) from the drop down list.

3 Perform one of the following.

a To create an RCA audit policy, click on the Create button. The Audit Policy (Create) form opens with the General tab displayed.

b To configure an existing RCA audit policy, click on the Search button and choose an entry from the list. Click on the Properties button. The Audit Policy (Edit) form opens with the General tab displayed. Go to step 5.

4 If you are creating an RCA audit policy, configure the following parameters. Otherwise, go to step 5.

- Auto-Assign ID
- ID

5 Configure the Description parameter.

6 If you are creating an RCA audit policy, click on the Select RCA Policy To Run The Audit button. Otherwise, go to step 11. The RCA Policy form opens.

7 Choose one of the following options:

- RCA Audit OSPF
- RCA Audit Physical Link
- RCA Audit ISIS
- RCA Audit VPRN
- RCA Audit VPLS
- Compare MME Instance
- RCA Audit VLL

Note 1 — You require a 5650 CPAM license to create an RCA Audit ISIS or RCA Audit OSPF policy.

Note 2 — See "9471 WMM golden configuration management" in the *5620 SAM LTE EPC User Guide* for information about performing golden configuration RCA audits on 9471 WMM instances.

8 Double-click on an entry to modify the policy description, if required.

9 Click on the OK button. The RCA Policy form closes.

10 Click on the Apply button.

11 Click on the Entry tab. Depending on the option specified in step 7, a list of RCA audit policy entries is displayed.

The RCA audit policy entry for a VLL RCA audit is: RCA Audit for VLL Service Membership.

The RCA audit policy entry for a VPRN RCA audit is: RCA Audit for VPRN Service Membership.

The following are the RCA audit policy entries for a VPLS RCA audit:

- RCA Audit for B-VPLS PBB
- RCA Audit for VPLS Service Membership
- RCA Audit for BGP Multi-homing
- RCA Audit for B-VPLS SPB

The following are the RCA audit policy entries for a physical link RCA audit:

- RCA Audit For Physical Ports of Physical Links
- RCA Audit For Ethernet Port Specifics of Physical Links

12 Choose an entry from the list and click on the Properties button. The Audit Policy Entry - RCA Audit Policy - RCA Audit For *Network_Object* (Edit) form opens with the General tab displayed.

13 Configure the parameters:

- Enabled
- Remove Empty Service

14 If you are configuring an RCA audit policy for physical links, perform the following steps. Otherwise, go to step 15.

i Click on the Attributes tab. A list of default attributes for the physical link entry is displayed.

ii Perform one of the following:

- To configure default attributes, go to step iii.
- To add an attribute, go to step v.

iii Activate or deactivate the RCA audit for each attribute by enabling or disabling the check box in the Enabled column.

iv Choose one of the problem severity options for each attribute by clicking on the entry in the Severity column of the attribute. A contextual menu appears.

- Minor
- Conditional
- Info
- Critical
- Major
- Warning
- Indeterminate

v Click on the Add button to add an attribute. Otherwise, go to step 15. The Adding new Attribute(s) - RCA Audit For *entry_type* of Physical Links form opens with a list of attributes associated with the physical link entry.

vi Choose one or more attributes in the list and click on the OK button. The Adding new Attribute(s) - RCA Audit For *entry_type* of Physical Links form closes and the Audit Policy Entry - RCA Audit Policy - RCA Audit For *entry_type* of Physical Links (Edit) form refreshes with the attribute information.

15 Click on the OK button. The Audit Policy Entry - RCA Audit Policy - RCA Audit For *Network_Object* (Edit) form closes.

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The Audit Policy (Edit) form closes.

18 Close the RCA Audits form.

Procedure 80-2 To perform an RCA audit of a VLL service

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and choose VLL from the object drop-down list.

3 Click on the Search button. A list of VLL services appears.

4 Choose an entry from the list and click on the Properties button. The *VLL_type* (Edit) form opens with the General tab displayed.

5 Check the following indicators:

- RCA Audit Problem(s)
- Last Audit Time

6 Click on the RCA Audit button. If the RCA Audit button is not visible, click on the More Actions button and choose RCA Audit. The Select RCA Policy list form appears with a list of configured policies.

7 Choose an entry and click on the OK button. The Select RCA Policy list form closes and a dialog box appears.

8 Click on the OK button.

9 Click on the RCA Result tab. The RCA audit information is displayed on the Related Problem tab.



Note — The RCA Result tab appears only if the RCA audit detects one or more problems.

10 If required, expand the VLL Service object in the problems tree to view the problems, the associated severity, and the cause.

11 Double-click on a problem icon to view information about the problem. The Problem (Edit) form opens with the General tab displayed. The following information is displayed:

- Last Time Changed
- Probable Cause
- Severity
- Description
- Solution

12 Configure the Disable Fix Window parameter.

13 Click on the Related Problem tab to view related problems.

14 Click on the Caused By Objects tab to view a list of objects that are causing the problem.

15 Choose an entry from the list and click on the Properties button. The properties form for the object opens.

16 Click on the tabs to view information about the configuration.

17 Configure the parameters, as required.

18 Click on the OK button to save the configuration and close the properties form. A dialog box appears.

19 Click on the Yes button.

20 Close the Problem (Edit) form.

21 To fix a problem:

i Click on the Related Problem tab.

ii Right-click on a problem icon and choose Fix Problem from the contextual menu. The Plan form appears.



Note — The Fix Problem menu option is disabled if you set the Disable Fix Window parameter to Enabled in step 12.

iii Check the recommended plan to fix the problem in the Plan panel.

iv Check the report about fixing the problem in the Report panel.

v Click on the Fix Problem button. The Plan form closes and a dialog box appears with a summary of the fix. Click on the OK button.

22 Close the *VLL_type* (Edit) form.

23 Close the Manage Services form.

Procedure 80-3 To perform an RCA audit of a VPLS

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Click on the Search button. A list of VPLS services appears.



Note 1 — In addition to the standard audit checks, for BGP VPLS multi-homing sites the audit also verifies:

- if no valid Route Targets are configured under a VPLS site that has BGP multi-homing sites configured under it.
- if there are no matching RTs for peered multi-homing sites
- if there are multiple RTs configured under a VPLS site that has BGP multi-homing sites configured under it. Multiple RTs will make the BGP multi-homing sites appear under multiple topologies (or multiple services, since the RT defines the service)
- if multi-homing sites have the same multi-homing ID but different RTs (different RTs mean the sites are in different topologies or services)
- if a multi-homing site does not have other sites as members (sharing the same multi-homing ID to comprise a group)

Note 2 — In addition to the standard audit checks, for SPB- enabled B-VPLS sites, the audit also verifies that:

- all user B-VPLS SAPs or spoke SDP bindings are fate-shared with a control B-VPLS
- control and user B-VPLS instances in the same service on different sites have the same FID
- FID-to-ECT mapping is consistent on all of the sites for the active SPB B-VPLS services
- control B-VPLS SPB level Unicast Forwarding Tree Topology parameter is consistent on all of the sites in the same service

3 Choose an entry from the list and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 Check the following indicators:

- RCA Audit Problem(s)
- Last Audit Time

5 Click on the RCA Audit button. If the RCA Audit button is not visible, click on the More Actions button and choose RCA Audit. The Select RCA Policy to run the audit list form appears with a list of configured policies.

6 Choose an entry and click on the OK button. The Select RCA Policy list form closes and the requested audit is performed. A dialog box appears.

7 Click on the OK button.

8 Click on the RCA Result tab. The RCA audit information is displayed on the Related Problem tab.



Note — The RCA Result tab appears only if the RCA audit detects one or more problems.

9 If required, expand the VPLS Service object in the problems tree to view the problems, the associated severity, and the cause.

10 Double-click on a problem icon to view information about the problem. The Problem (Edit) form opens with the General tab displayed. The following information is displayed:

- Last Time Changed
- Probable Cause
- Severity
- Description
- Solution

11 Configure the Disable Fix Window parameter.

12 Click on the Related Problem tab to view related problems.

13 Click on the Caused By Objects tab to view a list of objects that are causing the problem.

14 Choose an entry from the list and click on the Properties button. The properties form for the object opens.

15 Click on the tabs to view information about the configuration.

16 Configure the parameters, as required.

17 Click on the OK button to save the configuration and close the properties form. A dialog box appears.

18 Click on the Yes button.

19 Close the Problem (Edit) form.

20 To fix a problem:

i Click on the Related Problem tab.

ii Right-click on a problem icon and choose Fix Problem from the contextual menu. The Plan form appears.



Note — The Fix Problem menu option is disabled if you set the Disable Fix Window parameter to Enabled in step 11.

iii Check the recommended plan to fix the problem in the Plan panel.

iv Check the report about fixing the problem in the Report panel.

v Click on the Fix Problem button. The Plan form closes and a dialog box appears with a summary of the fix. Click on the OK button.

21 Close the VPLS Service (Edit) form.

22 Close the Manage Services form.

Procedure 80-4 To perform an RCA audit of a VPRN service

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and choose VPRN from the object drop-down list.

3 Click on the Search button. A list of VPRN services appears.

4 Choose an entry from the list and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

5 Check the following indicators:

- RCA Audit Problem(s)
- Last Audit Time

6 Click on the RCA Audit button. If the RCA Audit button is not visible, click on the More Actions button and choose RCA Audit. The Select RCA Policy list form appears with a list of configured policies.

7 Choose an entry and click on the OK button. The Select RCA Policy list form closes and a dialog box appears.

8 Click on the OK button.

9 Click on the RCA Result tab. The RCA audit information is displayed on the Related Problem tab.

Note — The RCA Result tab appears only if the RCA audit detects one or more problems.

10 If required, expand the VPRN Service object in the problems tree to view the problems, the associated severity, and the cause.

11 Double-click on a problem icon to view information about the problem. The Problem (Edit) form opens with the General tab displayed. The following information is displayed:

- Last Time Changed
- Probable Cause
- Severity
- Description
- Solution

12 Configure the Disable Fix Window parameter.

13 Click on the Related Problem tab to view related problems.

14 Click on the Caused By Objects tab to view a list of objects that are causing the problem.

15 Choose an entry from the list and click on the Properties button. The properties form for the object opens.

16 Click on the tabs to view information about the configuration.

17 Configure the parameters, as required.

18 Click on the OK button to save the configuration and close the properties form. A dialog box appears.

19 Click on the Yes button.

20 Close the Problem (Edit) form.

21 To fix a problem:

i Click on the Related Problem tab.

ii Right-click on a problem icon and choose Fix Problem from the contextual menu. The Plan form appears.

Note — The Fix Problem menu option is disabled if you set the Disable Fix Window parameter to Enabled in step 12.

iii Check the recommended plan to fix the problem in the Plan panel.

iv Check the report about fixing the problem in the Report panel.

v Click on the Fix Problem button. The Plan form closes and a dialog box appears with a summary of the fix. Click on the OK button.

22 Close the VPRN Service (Edit) form.

23 Close the Manage Services form.

Procedure 80-5 To perform an RCA audit of multiple services

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and choose one of the following from the Service (Management) object drop-down list.

- VPLS (VPLS)
- VPRN Service (VPRN)
- VLL (VLL)

3 Click on the Search button. A list of services appears.

4 Select the services that you want to audit.

5 Click on the RCA Audit button. The Select RCA Policy list form opens.

6 Choose an entry and click on the OK button. The Select RCA Policy list form closes and a dialog box appears with the following information:

- number of services audited
- number of successful audits
- number of problems generated

7 Click on the OK button.

8 Scroll to the RCA Audit Problem column and set the filter to = true.

9 Click on the Search button. A list of services with problems appears.

10 Select a service and click on the OK button. The *Service* (Edit) form appears with the General tab displayed.

11 Click on the RCA Result tab. The RCA audit information is displayed on the Related Problem tab.



Note — The RCA Result tab appears only if the RCA audit detects one or more problems.

12 If required, expand the *Service* object in the problems tree to view the problems, the associated severity, and the cause.

13 Double-click on a problem icon to view information about the problem. The Problem (Edit) form opens with the General tab displayed. The following information is displayed:

- Last Time Changed
- Probable Cause
- Severity
- Description
- Solution

14 Configure the Disable Fix Window parameter.

15 Click on the Related Problem tab to view related problems.

16 Click on the Caused By Objects tab to view a list of objects that are causing the problem.

17 Choose an entry from the list and click on the Properties button. The properties form for the object opens.

18 Click on the tabs to view information about the configuration.

19 Configure the parameters, as required.

20 Click on the OK button to save the configuration and close the properties form. A dialog box appears.

21 Click on the Yes button.

22 Close the Problem (Edit) form.

23 To fix a problem:

i Click on the Related Problem tab.

ii Right-click on a problem icon and choose Fix Problem from the contextual menu. The Plan form appears.



Note — The Fix Problem menu option is disabled if you set the Disable Fix Window parameter to Enabled in step 14.

iii Check the recommended plan to fix the problem in the Plan panel.

iv Check the report about fixing the problem in the Report panel.

v Click on the Fix Problem button. The Plan form closes and a dialog box appears with a summary of the fix. Click on the OK button.

24 Close the *Service* (Edit) form.

25 Close the Manage Services form.

Procedure 80-6 To perform an RCA audit of a physical link

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Click on the Select Object Type button and choose one of the following from the object tree.

- Physical Link (Network)
- Discovered Physical Link (Network)

3 Click on the Search button. A list of physical links appears.

4 Choose an entry from the list and click on the Properties button. The Physical Link (Edit) form opens with the General tab displayed.

5 Check the following indicators:

- RCA Audit Problem(s)
- Last Audit Time

6 Click on the RCA Audit button. If the RCA Audit button is not visible, click on the More Actions button and choose RCA Audit. The Select RCA Policy list form appears with a list of configured policies.

7 Choose an entry and click on the OK button. The Select RCA Policy list form closes and a dialog box appears.

8 Click on the OK button.

9 Click on the RCA Result tab. The RCA audit information is displayed on the Related Problem tab.



Note — The RCA Result tab appears only if the RCA audit detects one or more problems.

10 If required, expand the Physical Link object in the problems tree to view the problems, the associated severity, and the cause.

11 Double-click on a problem icon to view information about the problem. The Problem (Edit) form opens with the General tab displayed. The following information is displayed:

- Last Time Changed
- Probable Cause
- Severity
- Description
- Solution

12 Click on the Related Problem tab to view related problems.



Note — The 5620 SAM does not provide a solution for physical link configuration errors.

13 Click on the Caused By Objects tab to view a list of objects that are causing the problem.

14 Choose an entry from the list and click on the Properties button. The properties form for the object opens.

15 Click on the tabs to view information about the configuration.

16 Configure the parameters, as required.

17 Click on the OK button to save the configuration and close the properties form. A dialog box appears.

18 Click on the Yes button.

19 Close the Problem (Edit) form.

20 Close the Physical Link (Edit) form.

21 Close the Manage Equipment form.

Procedure 80-7 To create a service audit scheduled task

1 Choose Policies→RCA Audits from the 5620 SAM main menu. The RCA Audits form opens.

2 Specify a filter for the search, if required, and click on the Search button. A list of RCA audit policies appears.

3 Choose a service audit policy from the list and click on the Properties button. The Audit Policy (Edit) form opens with the General tab displayed.

4 Click on the Schedule button and choose Create RCA Audit Schedule Task. The Service Audit Scheduled Task (Create) form opens.

5 Configure the parameters:

- Scheduled Task Name
- Scheduled Task Description
- Administrative State

6 Click on the Select button in the Schedule panel. The Select Schedule - Service Audit Scheduled Task form opens.

7 Perform one of the following.

a Create a schedule to associate with the scheduled task.

b Associate an existing schedule to the scheduled task. Go to step 9.

8 Create a schedule.

i Configure the parameters:

- Name
- Description
- Current Client Start Time
- Current Client End Time
- Delay Time (seconds)
- Enable
- Ongoing
- Frequency

The Current Client End Time parameter is configurable when the Ongoing parameter is disabled and the Frequency parameter value is set to something other than Once.

When a SAM Schedule is not Ongoing and is assigned to a task, the 5620 SAM raises an alarm when the Current Client End Time expires.

ii Perform the step that corresponds to the Frequency parameter value specified in step i.

- When the parameter is set to Once, go to step iii.
- When the parameter is set to Per Second, configure the following parameters:
  - Run Every Second
  - Run Every Seconds
- When the parameter is set to Per Minute, configure the following parameters:
  - Run Every Minute
  - Run Every Minutes
- When the parameter is set to Per Hour, configure the following parameters:
  - Run Every Hour
  - Run Every Hours
- When the parameter is set to Per Day, configure the following parameters:
  - Run Every Day
  - Run Every Days
  - Run Every
- When the parameter is set to Per Week, configure the following parameters:



Note — The Run Every parameter is not configurable when the Ongoing parameter is enabled.

  - Run Every Week
  - Run Every Weeks
  - Run Every
- When the parameter is set to Per Month, configure the following parameters:



Note — The Run Every parameter is not configurable when the Ongoing parameter is enabled.

  - Run Every Month
  - Run Every Months
  - Run Every

iii Click on the OK button to save the changes. The SAM Schedule (Create) form closes and the Select Schedule - Service Audit Scheduled Task form reappears.

9 Choose an entry from the list and click on the OK button. The Select Schedule - Service Audit Scheduled Task form closes and the Service Audit Scheduled Task (Create) form reappears.

10 Ensure that the Administrative State parameter is set to Enabled.

11 Click on the OK button. The Service Audit Scheduled Task (Create) form closes. The RCA Audit Policy form reappears with additional tabs.

12 To apply a filter to the schedule, perform the following.

i Click on the Schedule Filter tab.

ii Click on the Select button in the Audit Filter panel. The Select Audit Filter - Audit Policy form opens.

iii Click on the Search button. A list of filters appears.



Note — If no filters appear, click on the Audit Filter button to create a new filter. See chapter 3 for more information about how to create a filter.

iv Choose an entry and click on the OK button. The Select Audit Filter - Audit Policy form closes and the Audit Policy (Edit) form reappears with additional tabs.

13 Click on the Scheduled Objects to be Audited tab to view the services that are included in the audit.

14 Click on the Scheduled Result tab to view the results of the scheduled audit.

15 Click on the Problems tab to view the problems associated with the audit.

16 Close the Audit Policy (Edit) form.

17 Close the RCA Audits form.

81 — Service throughput configuration

81.1 Service throughput configuration overview *81-2*

81.2 Workflow to prepare for and restore from a service throughput configuration *81-2*

81.3 Service throughput configuration procedures *81-3*

81.1 Service throughput configuration overview

The 5620 SAM allows you to create a copy of the SAP configuration of an end-user service that emulates the bandwidth, throughput, and QoS requirements of the service. You can perform any required OAM diagnostics on the service while sending the traffic through the NEs, to compare the customer SLA with current measurements and report the results.

Throughput configurations are supported on the 7210 SAS, 7705 SAR and 7750 SR, and on VLL Epipe, VPLS, and composite services that contain an Epipe and VPLS, or both. You can create a SAP based on the configuration of an existing SAP to prepare the service throughput configuration, where the port under the new SAP connects to the test entry or a loopback port as the destination.

Consider the following when you prepare a throughput test environment:

- The SAP to be replaced must reside under a Epipe site, including PBB Epipes, or a VPLS site including I-VPLS and B-VPLS.
- The following SAPs are not supported for the throughput test:
  - CCAGs
  - LAGs
  - SAPs that reside on an Ethernet tunnel element
  - SAPs that reside on an Ethernet ring element
  - SAPs used by a mirror service
- E-OAM objects, such as MEPs, are not copied to the test SAP.

You can view existing service throughput configurations on the Throughput Configuration tab of a service. Services and sites with a service throughput configuration have the Modified for Throughput Test parameter enabled on the General tab of the service or site.

81.2 Workflow to prepare for and restore from a service throughput configuration

The following workflow describes the high-level tasks required to prepare a throughput configuration. The workflow assumes that a 5620 SAM end user is challenging the offered SLA.

1. Open the service on which you need to create the test environment.
2. Set the Current OLC State parameter to Maintenance.
3. Prepare the configuration. See Procedure 81-1.
4. Perform OAM diagnostics, as required. See chapter 77 for more information about the 5620 SAM service test manager.
5. Restore the service to the original configuration. See Procedure 81-2.
6. Set the Current OLC State parameter to In Service.

81.3 Service throughput configuration procedures

Use the following procedures to prepare for and restore from a 5620 SAM service throughput configuration SAP configuration.

Procedure 81-1 To prepare a service throughput configuration

Perform the following procedure to create a throughput configuration to prepare a throughput configuration on an Epipe or VPLS.



Note 1 — The SAP that is replaced for the throughput configuration must exist under an Epipe or VPLS site. A throughput configuration cannot be performed on a SAP that:

- resides on CCAG or LAG
- resides on Ethernet tunnel element
- resides on Ethernet ring element
- is used by a mirror service

Note 2 — Alcatel-Lucent recommends that you set the Current OLC State parameter of the service to Maintenance before you prepare a throughput configuration. See Procedures 67-1 and 68-1.

1 Perform one of the following:

   a To prepare a service throughput configuration on an Epipe or VPLS, choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

   b To prepare a service throughput configuration on a composite service, choose Manage→Service→Composite Services from the 5620 SAM main menu. The Manage Composite Services form opens.

2 Specify a filter for the search, if required, and click on the Search button. A list of services appears.

3 Perform one of the following:

   a Choose a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

   b Choose a VLL Epipe and click on the Properties button. The Epipe Service (Edit) form opens with the General tab displayed.

   c Choose a composite service and click on the Properties button. The Composite Service (Edit) form opens with the General tab displayed.

4 In the Throughput Configuration tab, click on the Create button. The Throughput Configuration form opens.



Note — Alternatively, you can choose a service throughput-capable service from the Manage Services or Manage Composite Services form, click on the Throughput Configuration button, and choose Create from the contextual menu.

5 Choose the entry SAP to be replaced for testing.

i Click on the Select button beside the SAP parameter in the Traffic Test Entry panel. The Select SAP - Throughput Configuration form opens with a list of L2 access interfaces configured in the service.

ii Choose a SAP and click on the OK button. The Select SAP - Throughput Configuration form closes and the Throughput Configuration form refreshes with the SAP information.

6 Specify a physical port or channel that is connected to the test entry and has the same encapsulation type as the SAP that you selected in step 5, on which to create the SAP. By default, the displayed port is the underlying port of the selected SAP. If you choose a different port, the 5620 SAM creates a SAP on the selected port by copying the configuration from the original SAP during the test preparation. E-OAM objects are not copied to the SAP.

i Click on the Select button beside the Port parameter in the Traffic Test Entry panel. The Select Port - Throughput Configuration form opens with a list of access or hybrid ports on the service site on which the SAP that you selected in step 5 resides, and that have the same encapsulation type as the selected SAP.

ii Choose a port and click on the OK button. The Select Port - Throughput Configuration form closes and the Throughput Configuration form refreshes with the port information.

7 Perform the following to choose the traffic destination site.

i Click on the Select button beside the Site ID parameter in the Traffic Test Destination panel. The Select Site ID - Service Throughput Configuration form opens with a list of sites configured in the service that support throughput configuration.

ii Choose a site and click on the OK button. The Select Site ID - Service Throughput Configuration form closes and the Throughput Configuration form refreshes with the site information.

8 Perform one of the following to configure the behavior for the traffic destination:

a To replace an existing SAP with a new SAP on a different port, set the Option parameter to Swap SAP and go to step 9.

b To loopback a port used by an existing SAP, set the Option parameter to Loopback Port Used By SAP and go to step 10.

c To replace an existing SAP with a new SAP on a different port and loopback the new port, set the Option parameter to Swap SAP and Loopback New Port and go to step 11.

d To loopback an existing SAP, set the Option parameter to Loopback SAP and go to step 12.

e To loopback an existing SDP binding, set the Option parameter to Loopback SDP Binding and go to step 13.



Note — The available options change depending on the node where the traffic destination site is configured.

9 Choose the destination SAP and port by performing the following:

i Click on the Select button beside the SAP parameter in the Traffic Test Destination panel. The Select SAP - Service Throughput Configuration form appears with a list of L2 access interfaces configured on the service.

ii Choose a SAP and click on the OK button.

iii Click on the Select button beside the Port parameter in the Traffic Test Destination panel. The Select Port - Service Throughput Configuration form appears with a list of ports on the same site as the selected SAP.

iv Choose the port that you need to swap to and click on the OK button. The port must have the same encapsulation type as the selected SAP.

v Go to step 15.

10 Choose the destination SAP and configure loopback parameters on the port by performing the following:

i Click on the Select button beside the SAP parameter in the Traffic Test Destination panel. The Select SAP - Service Throughput Configuration form appears with a list of L2 access interfaces configured on the service.

ii Choose a SAP and click on the OK button.

iii Configure the parameters. The available parameters change depending on the node where the destination SAP is configured, and include the following:

- Loopback SAP
- Loopback Type
- Loopback Time
- Swap MAC Address
- Source MAC Address
- Destination MAC Address

iv Go to step 15.

11 Choose the destination SAP and loopback port, and configure parameters on the port by performing the following:

i Click on the Select button beside the SAP parameter in the Traffic Test Destination panel. The Select SAP - Service Throughput Configuration form appears with a list of L2 access interfaces configured on the service.

ii Choose a SAP and click on the OK button.

iii Click on the Select button beside the Port parameter in the Traffic Test Destination panel. The Select Port - Service Throughput Configuration form appears with a list of ports on the same site as the selected SAP.

iv Choose the port that you need to swap to and click on the OK button. The port must have the same encapsulation type as the selected SAP.

v Configure the parameters. The available parameters change depending on the node where the destination SAP is configured, and include the following:

- Loopback SAP
- Loopback Type
- Loopback Time
- Swap MAC Address
- Source MAC Address
- Destination MAC Address

vi Go to step 15.

12 Choose the destination SAP and configure loopback parameters by performing the following:

i Click on the Select button beside the SAP parameter in the Loopback SAP panel. The Select SAP - Service Throughput Configuration form appears with a list of L2 access interfaces configured on the destination site.

ii Choose a SAP and click on the OK button.

iii Configure the loopback parameters:

- Loopback Mode
- MAC Swap
- MAC Swap Address
- MAC Swap Address All

iv Go to step 15.

13 Choose an SDP binding and configure loopback parameters by performing the following:

i Click on the Select button beside the Destination Site parameter in the Loopback SDP Binding panel. The Select SDP Binding - Service Throughput Configuration form appears with a list of supported SDP bindings configured on the destination site.

ii Choose an SDP binding and click on the OK button.

iii Configure the loopback parameters:

- Loopback Mode
- MAC Swap
- MAC Swap Address
- MAC Swap Address All

iv Go to step 15.

14 Click on the OK button. The Service Throughput Configuration form closes.

15 Click on the Apply button on the VPLS Service (Edit) form to perform the following, if applicable:

- create a SAP on the selected port if the selected port differs from the port on the SAP
- configure the SAP with the same configuration as the original SAP, including all child objects that are copied over to the SAP
- delete the original SAP
- propagate port loopback parameter changes to the test port
- change the test SAP to a loopback SAP with the configured loopback parameters
- change the test SDP binding to a loopback SDP binding with the configured loopback parameters
- update the throughput information on the site
- update the throughput information on the service



Note — A site can only be used in one throughput configuration at a time. If a throughput configuration exists that uses a site as either a source or a destination, that site cannot be used in another throughput configuration.

16 Perform OAM diagnostics as required.

17 Close the VPLS Service (Edit) form or the Epipe Service (Edit) form.

18 Close the Manage Services form.

Procedure 81-2 To restore a service after a throughput configuration

The 5620 SAM performs the following when you restore the service:

- deletes the newly created SAPs
- re-creates the original SAPs
- on the loopback port: resets the loopback type to none if it was changed by the throughput configuration, and changes the loopback parameters to their default values

- updates the site throughput status information
- updates the service throughput status information

1 Perform one of the following:

   a Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

   b Choose Manage→Service→Composite Services from the 5620 SAM main menu. The Manage Services form opens.

2 Specify a filter for the search, if required, and click on the Search button. A list of services appears.

3 Choose the service for which you need to restore the configuration and click on the Properties button. The *Service_type* Service (Edit) form opens with the General tab displayed.

4 Click on the Throughput Configuration tab. A list of throughput configurations on the service appears.

5 Select the throughput configuration you need to remove, and click on the Delete button.



Note — Alternatively, you can select a service or composite service that is modified for throughput configuration from the Manage Services form or Manage Composite Services, click on the Throughput Configuration button, and choose Delete (all) from the contextual menu. This removes all the service throughput configurations on the service.

6 Close the *Service_type* Service (Edit) form.

7 Close the Manage Services form.

Customer documentation and product support



Customer documentation

http://www.alcatel-lucent.com/myaccess

Product manuals and documentation updates are available at alcatel-lucent.com. If you are a new user and require access to this service, please contact your Alcatel-Lucent sales representative.



Technical Support

http://support.alcatel-lucent.com



Documentation feedback

documentation.feedback@alcatel-lucent.com



© 2013-2015 Alcatel-Lucent. All rights reserved.

3HE 08041 AAAH TQZZA Edition 01