# Cisco IOS Mobile Wireless Home Agent Configuration Guide

Release 12.4T

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

*Cisco IOS Mobile Wireless Home Agent Configuration Guide*

# About Cisco IOS and Cisco IOS XE Software Documentation

**Last updated: August 6, 2008**

This document describes the objectives, audience, conventions, and organization used in Cisco IOS and Cisco IOS XE software documentation, collectively referred to in this document as Cisco IOS documentation. Also included are resources for obtaining technical assistance, additional documentation, and other information from Cisco. This document is organized into the following sections:



## Documentation Objectives

Cisco IOS documentation describes the tasks and commands available to configure and maintain Cisco networking devices.

## Audience

The Cisco IOS documentation set is i ntended for users who configure and maintain Cisco networking devices (such as routers and switches) but who may not be familiar with the configuration and maintenance tasks, the relationship among tasks, or the Cisco IOS commands necessary to perform particular tasks. The Cisco IOS documentation set is also intended for those users experienced with Cisco IOS who need to know about new features, new configuration options, and new software characteristics in the current Cisco IOS release.

# Documentation Conventions

In Cisco IOS documentation, the term *router* may be used to refer to various Cisco products; for example, routers, access servers, and switches. These and other networking devices that support Cisco IOS software are shown interchangeably in examples and are used only for illustrative purposes. An example that shows one product does not necessarily mean that other products are not supported.

This section includes the following topics:



## Typographic Conventions

Cisco IOS documentation uses the following typographic conventions:

| Convention | Description |
|---|---|
| ^ or Ctrl | Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.) |
| *string* | A string is a nonquoted set of characters shown in italics. For example, when setting a Simple Network Management Protocol (SNMP) community string to *public*, do not use quotation marks around the string; otherwise, the string will include the quotation marks. |

## Command Syntax Conventions

Cisco IOS documentation uses the following command syntax conventions:

| Convention | Description |
|---|---|
| **bold** | Bold text indicates commands and keywords that you enter as shown. |
| *italic* | Italic text indicates arguments for which you supply values. |
| [x] | Square brackets enclose an optional keyword or argument. |
| \| | A vertical line, called a pipe, indicates a choice within a set of keywords or arguments. |
| [x \| y] | Square brackets enclosing keywords or arguments separated by a pipe indicate an optional choice. |
| {x \| y} | Braces enclosing keywords or arguments separated by a pipe indicate a required choice. |
| [x {y \| z}] | Braces and a pipe within square brackets indicate a required choice within an optional element. |

## Software Conventions

Cisco IOS uses the following program code conventions:

| Convention | Description |
|---|---|
| `Courier font` | Courier font is used for information that is displayed on a PC or terminal screen. |
| **`Bold Courier font`** | Bold Courier font indicates text that the user must enter. |
| < > | Angle brackets enclose text that is not displayed, such as a password. Angle brackets also are used in contexts in which the italic font style is not supported; for example, ASCII text. |
| ! | An exclamation point at the beginning of a line indicates that the text that follows is a comment, not a line of code. An exclamation point is also displayed by Cisco IOS software for certain processes. |
| [ ] | Square brackets enclose default responses to system prompts. |

## Reader Alert Conventions

The Cisco IOS documentation set uses the following conventions for reader alerts:

**Caution** Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

**Note** Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

**Timesaver** Means *the described action saves time*. You can save time by performing the action described in the paragraph.

# Documentation Organization

This section describes the Cisco IOS documentation set, how it is organized, and how to access it on Cisco.com. Included are lists of configuration guides, command references, and supplementary references and resources that make up the documentation set. The following topics are included:

# Cisco IOS Documentation Set

Cisco IOS documentation consists of the following:

- Release notes and caveats provide information about platform, technology, and feature support for a release and describe severity 1 (catastrophic), severity 2 (severe), and severity 3 (moderate) defects in released Cisco IOS code. Review release notes before other documents to learn whether or not updates have been made to a feature.
- Sets of configuration guides and command references organized by technology and published for each standard Cisco IOS release.
  - Configuration guides—Compilations of documents that provide informational and task-oriented descriptions of Cisco IOS features.
  - Command references—Compilations of command pages that provide detailed information about the commands used in the Cisco IOS features and processes that make up the related configuration guides. For each technology, there is a single command reference that covers all Cisco IOS releases and that is updated at each standard release.
- Lists of all the commands in a specific release and all commands that are new, modified, removed, or replaced in the release.
- Command reference book for **debug** commands. Command pages are listed in alphabetical order.
- Reference book for system messages for all Cisco IOS releases.

# Cisco IOS Documentation on Cisco.com

The following sections describe the documentation organization and how to access various document types.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

### New Features List

The New Features List for each release provides a list of all features in the release with hyperlinks to the feature guides in which they are documented.

### Feature Guides

Cisco IOS features are documented in feature guides. Feature guides describe one feature or a group of related features that are supported on many different software releases and platforms. Your Cisco IOS software release or platform may not support all the features documented in a feature guide. See the Feature Information table at the end of the feature guide for information about which features in that guide are supported in your software release.

### Configuration Guides

Configuration guides are provided by technology and release and comprise a set of individual feature guides relevant to the release and technology.

### Command References

Command reference books describe Cisco IOS commands that are supported in many different software releases and on many different platforms. The books are provided by technology. For information about all Cisco IOS commands, use the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or the *Cisco IOS Master Command List, All Releases*, at http://www.cisco.com/en/US/docs/ios/mcl/all_release/all_mcl.html.

### Cisco IOS Supplementary Documents and Resources

Supplementary documents and resources are listed in Table 2 on page xi.

# Configuration Guides, Command References, and Supplementary Resources

Table 1 lists, in alphabetical order, Cisco IOS and Cisco IOS XE software configuration guides and command references, including brief descriptions of the contents of the documents. The Cisco IOS command references are comprehensive, meaning that they include commands for both Cisco IOS software and Cisco IOS XE software, for all releases. The configuration guides and command references support many different software releases and platforms. Your Cisco IOS software release or platform may not support all these technologies.

For additional information about configuring and operating specific networking devices, go to the Product Support area of Cisco.com at http://www.cisco.com/web/psa/products/index.html.

Table 2 lists documents and resources that supplement the Cisco IOS software configuration guides and command references. These supplementary resources include release notes and caveats; master command lists; new, modified, removed, and replaced command lists; system messages; and the debug command reference.

***Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References***

| Configuration Guide and Command Reference Titles | Features/Protocols/Technologies |
|---|---|
| *Cisco IOS AppleTalk Configuration Guide*<br>*Cisco IOS XE AppleTalk Configuration Guide*<br>*Cisco IOS AppleTalk Command Reference* | AppleTalk protocol. |
| *Cisco IOS Asynchronous Transfer Mode Configuration Guide*<br>*Cisco IOS Asynchronous Transfer Mode Command Reference* | LAN ATM, multiprotocol over ATM (MPoA), and WAN ATM. |

*Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)*

| Configuration Guide and Command Reference Titles | Features/Protocols/Technologies |
|---|---|
| *Cisco IOS Bridging and IBM Networking Configuration Guide*<br>*Cisco IOS Bridging Command Reference*<br>*Cisco IOS IBM Networking Command Reference* | • Transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and token ring route switch module (TRRSM).<br>• Data-link switching plus (DLSw+), serial tunnel (STUN), block serial tunnel (BSTUN); logical link control, type 2 (LLC2), synchronous data link control (SDLC); IBM Network Media Translation, including Synchronous Data Logical Link Control (SDLLC) and qualified LLC (QLLC); downstream physical unit (DSPU), Systems Network Architecture (SNA) service point, SNA frame relay access, advanced peer-to-peer networking (APPN), native client interface architecture (NCIA) client/server topologies, and IBM Channel Attach. |
| *Cisco IOS Broadband and DSL Configuration Guide*<br>*Cisco IOS XE Broadband and DSL Configuration Guide*<br>*Cisco IOS Broadband and DSL Command Reference* | Point-to-Point Protocol (PPP) over ATM (PPPoA) and PPP over Ethernet (PPPoE). |
| *Cisco IOS Carrier Ethernet Configuration Guide*<br>*Cisco IOS Carrier Ethernet Command Reference* | Connectivity fault management (CFM), Ethernet Local Management Interface (ELMI), IEEE 802.3ad link bundling, Link Layer Discovery Protocol (LLDP), media endpoint discovery (MED), and operations, administration, and maintenance (OAM). |
| *Cisco IOS Configuration Fundamentals Configuration Guide*<br>*Cisco IOS XE Configuration Fundamentals Configuration Guide*<br>*Cisco IOS Configuration Fundamentals Command Reference* | Autoinstall, Setup, Cisco IOS command-line interface (CLI), Cisco IOS file system (IFS), Cisco IOS web browser user interface (UI), basic file transfer services, and file management. |
| *Cisco IOS DECnet Configuration Guide*<br>*Cisco IOS XE DECnet Configuration Guide*<br>*Cisco IOS DECnet Command Reference* | DECnet protocol. |
| *Cisco IOS Dial Technologies Configuration Guide*<br>*Cisco IOS XE Dial Technologies Configuration Guide*<br>*Cisco IOS Dial Technologies Command Reference* | Asynchronous communications, dial backup, dialer technology, dial-in terminal services and AppleTalk remote access (ARA), large scale dialout, dial-on-demand routing, dialout, modem and resource pooling, ISDN, multilink PPP (MLP), PPP, virtual private dialup network (VPDN). |
| *Cisco IOS Flexible NetFlow Configuration Guide*<br>*Cisco IOS Flexible NetFlow Command Reference* | Flexible NetFlow. |

*Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)*

| Configuration Guide and Command Reference Titles | Features/Protocols/Technologies |
|---|---|
| *Cisco IOS H.323 Configuration Guide* | Gatekeeper enhancements for managed voice services, Gatekeeper Transaction Message Protocol, gateway codec order preservation and shutdown control, H.323 dual tone multifrequency relay, H.323 version 2 enhancements, Network Address Translation (NAT) support of H.323 v2 Registration, Admission, and Status (RAS) protocol, tokenless call authorization, and VoIP gateway trunk and carrier-based routing. |
| *Cisco IOS High Availability Configuration Guide*<br>*Cisco IOS XE High Availability Configuration Guide*<br>*Cisco IOS High Availability Command Reference* | A variety of High Availability (HA) features and technologies that are available for different network segments (from enterprise access to service provider core) to facilitate creation of end-to-end highly available networks. Cisco IOS HA features and technologies can be categorized in three key areas: system-level resiliency, network-level resiliency, and embedded management for resiliency. |
| *Cisco IOS Integrated Session Border Controller Command Reference* | A VoIP-enabled device that is deployed at the edge of networks. An SBC is a toolkit of functions, such as signaling interworking, network hiding, security, and quality of service (QoS). |
| *Cisco IOS Intelligent Service Gateway Configuration Guide*<br>*Cisco IOS Intelligent Service Gateway Command Reference* | Subscriber identification, service and policy determination, session creation, session policy enforcement, session life-cycle management, accounting for access and service usage, session state monitoring. |
| *Cisco IOS Interface and Hardware Component Configuration Guide*<br>*Cisco IOS XE Interface and Hardware Component Configuration Guide*<br>*Cisco IOS Interface and Hardware Component Command Reference* | LAN interfaces, logical interfaces, serial interfaces, virtual interfaces, and interface configuration. |
| *Cisco IOS IP Addressing Services Configuration Guide*<br>*Cisco IOS XE Addressing Services Configuration Guide*<br>*Cisco IOS IP Addressing Services Command Reference* | Address Resolution Protocol (ARP), Network Address Translation (NAT), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Next Hop Address Resolution Protocol (NHRP). |
| *Cisco IOS IP Application Services Configuration Guide*<br>*Cisco IOS XE IP Application Services Configuration Guide*<br>*Cisco IOS IP Application Services Command Reference* | Enhanced Object Tracking (EOT), Gateway Load Balancing Protocol (GLBP), Hot Standby Router Protocol (HSRP), IP Services, Server Load Balancing (SLB), Stream Control Transmission Protocol (SCTP), TCP, Web Cache Communication Protocol (WCCP), User Datagram Protocol (UDP), and Virtual Router Redundancy Protocol (VRRP). |
| *Cisco IOS IP Mobility Configuration Guide*<br>*Cisco IOS IP Mobility Command Reference* | Mobile ad hoc networks (MANet) and Cisco mobile networks. |
| *Cisco IOS IP Multicast Configuration Guide*<br>*Cisco IOS XE IP Multicast Configuration Guide*<br>*Cisco IOS IP Multicast Command Reference* | Protocol Independent Multicast (PIM) sparse mode (PIM-SM), bidirectional PIM (bidir-PIM), Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), Internet Group Management Protocol (IGMP), and Multicast VPN (MVPN). |

*Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)*

| Configuration Guide and Command Reference Titles | Features/Protocols/Technologies |
|---|---|
| *Cisco IOS IP Routing Protocols Configuration Guide*<br>*Cisco IOS XE IP Routing Protocols Configuration Guide*<br>*Cisco IOS IP Routing Protocols Command Reference* | Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast, bidirectional forwarding detection (BFD), Enhanced Interior Gateway Routing Protocol (EIGRP), Interior Gateway Routing Protocol (IGRP), Intermediate System-to-Intermediate System (IS-IS), on-demand routing (ODR), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP). |
| *Cisco IOS IP SLAs Configuration Guide*<br>*Cisco IOS XE IP SLAs Configuration Guide*<br>*Cisco IOS IP SLAs Command Reference* | Cisco IOS IP Service Level Agreements (IP SLAs). |
| *Cisco IOS IP Switching Configuration Guide*<br>*Cisco IOS XE IP Switching Configuration Guide*<br>*Cisco IOS IP Switching Command Reference* | Cisco Express Forwarding, fast switching, and Multicast Distributed Switching (MDS). |
| *Cisco IOS IPv6 Configuration Guide*<br>*Cisco IOS XE IPv6 Configuration Guide*<br>*Cisco IOS IPv6 Command Reference* | For IPv6 features, protocols, and technologies, go to the IPv6 "Start Here" document at the following URL:<br>http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html |
| *Cisco IOS ISO CLNS Configuration Guide*<br>*Cisco IOS XE ISO CLNS Configuration Guide*<br>*Cisco IOS ISO CLNS Command Reference* | ISO connectionless network service (CLNS). |
| *Cisco IOS LAN Switching Configuration Guide*<br>*Cisco IOS XE LAN Switching Configuration Guide*<br>*Cisco IOS LAN Switching Command Reference* | VLANs, Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, IEEE 802.1Q encapsulation, and multilayer switching (MLS). |
| *Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide*<br>*Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference* | Cisco IOS Gateway GPRS Support Node (GGSN) in a 2.5-generation general packet radio service (GPRS) and 3-generation universal mobile telecommunication system (UMTS) network. |
| *Cisco IOS Mobile Wireless Home Agent Configuration Guide*<br>*Cisco IOS Mobile Wireless Home Agent Command Reference* | Cisco Mobile Wireless Home Agent, an anchor point for mobile terminals for which mobile IP or proxy mobile IP services are provided. |
| *Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide*<br>*Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference* | Cisco Packet Data Serving Node (PDSN), a wireless gateway that is between the mobile infrastructure and standard IP networks and that enables packet data services in a code division multiple access (CDMA) environment. |
| *Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide*<br>*Cisco IOS Mobile Wireless Radio Access Networking Command Reference* | Cisco IOS radio access network products. |

*Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)*

| Configuration Guide and Command Reference Titles | Features/Protocols/Technologies |
|---|---|
| *Cisco IOS Multiprotocol Label Switching Configuration Guide*<br>*Cisco IOS XE Multiprotocol Label Switching Configuration Guide*<br>*Cisco IOS Multiprotocol Label Switching Command Reference* | MPLS Label Distribution Protocol (LDP), MPLS Layer 2 VPNs, MPLS Layer 3 VPNs, MPLS Traffic Engineering (TE), and MPLS Embedded Management (EM) and MIBs. |
| *Cisco IOS Multi-Topology Routing Configuration Guide*<br>*Cisco IOS Multi-Topology Routing Command Reference* | Unicast and multicast topology configurations, traffic classification, routing protocol support, and network management support. |
| *Cisco IOS NetFlow Configuration Guide*<br>*Cisco IOS XE NetFlow Configuration Guide*<br>*Cisco IOS NetFlow Command Reference* | Network traffic data analysis, aggregation caches, export features. |
| *Cisco IOS Network Management Configuration Guide*<br>*Cisco IOS XE Network Management Configuration Guide*<br>*Cisco IOS Network Management Command Reference* | Basic system management; system monitoring and logging; troubleshooting, logging, and fault management; Cisco Discovery Protocol; Cisco IOS Scripting with Tool Control Language (Tcl); Cisco networking services (CNS); DistributedDirector; Embedded Event Manager (EEM); Embedded Resource Manager (ERM); Embedded Syslog Manager (ESM); HTTP; Remote Monitoring (RMON); SNMP; and VPN Device Manager Client for Cisco IOS Software (XSM Configuration). |
| *Cisco IOS Novell IPX Configuration Guide*<br>*Cisco IOS XE Novell IPX Configuration Guide*<br>*Cisco IOS Novell IPX Command Reference* | Novell Internetwork Packet Exchange (IPX) protocol. |
| *Cisco IOS Optimized Edge Routing Configuration Guide*<br>*Cisco IOS Optimized Edge Routing Command Reference* | Optimized edge routing (OER) monitoring, policy configuration, routing control, logging and reporting, and VPN IPsec/generic routing encapsulation (GRE) tunnel interface optimization. |
| *Cisco IOS Quality of Service Solutions Configuration Guide*<br>*Cisco IOS XE Quality of Service Solutions Configuration Guide*<br>*Cisco IOS Quality of Service Solutions Command Reference* | Class-based weighted fair queuing (CBWFQ), custom queuing, distributed traffic shaping (DTS), generic traffic shaping (GTS), IP- to-ATM class of service (CoS), low latency queuing (LLQ), modular QoS CLI (MQC), Network-Based Application Recognition (NBAR), priority queuing, Security Device Manager (SDM), Multilink PPP (MLPPP) for QoS, header compression, AutoQoS, QoS features for voice, Resource Reservation Protocol (RSVP), weighted fair queuing (WFQ), and weighted random early detection (WRED). |
| *Cisco IOS Security Configuration Guide*<br>*Cisco IOS XE Security Configuration Guide*<br>*Cisco IOS Security Command Reference* | Access control lists (ACLs), authentication, authorization, and accounting (AAA), firewalls, IP security and encryption, neighbor router authentication, network access security, network data encryption with router authentication, public key infrastructure (PKI), RADIUS, TACACS+, terminal access security, and traffic filters. |

*Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)*

| Configuration Guide and Command Reference Titles | Features/Protocols/Technologies |
|---|---|
| *Cisco IOS Service Selection Gateway Configuration Guide*<br>*Cisco IOS Service Selection Gateway Command Reference* | Subscriber authentication, service access, and accounting. |
| *Cisco IOS Software Activation Configuration Guide*<br>*Cisco IOS Software Activation Command Reference* | An orchestrated collection of processes and components to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses. |
| *Cisco IOS Software Modularity Installation and Configuration Guide*<br>*Cisco IOS Software Modularity Command Reference* | Installation and basic configuration of software modularity images, including installations on single and dual route processors, installation rollbacks, software modularity binding, software modularity processes and patches. |
| *Cisco IOS Terminal Services Configuration Guide*<br>*Cisco IOS Terminal Services Command Reference*<br>*Cisco IOS XE Terminal Services Command Reference* | DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD). |
| *Cisco IOS Virtual Switch Command Reference* | Virtual switch redundancy, high availability, and packet handling; converting between standalone and virtual switch modes; virtual switch link (VSL); Virtual Switch Link Protocol (VSLP).<br>**Note** For information about virtual switch configuration, refer to the product-specific software configuration information for the Cisco Catalyst 6500 series switch or for the Metro Ethernet 6500 series switch. |
| *Cisco IOS Voice Configuration Library*<br>*Cisco IOS Voice Command Reference* | Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. The library includes documentation for IP telephony applications. |
| *Cisco IOS VPDN Configuration Guide*<br>*Cisco IOS XE VPDN Configuration Guide*<br>*Cisco IOS VPDN Command Reference* | Layer 2 Tunneling Protocol (L2TP) dial-out load balancing and redundancy, L2TP extended failover, L2TP security VPDN, multihop by Dialed Number Identification Service (DNIS), timer and retry enhancements for L2TP and Layer 2 Forwarding (L2F), RADIUS Attribute 82: tunnel assignment ID, shell-based authentication of VPDN users, tunnel authentication via RADIUS on tunnel terminator. |
| *Cisco IOS Wide-Area Networking Configuration Guide*<br>*Cisco IOS XE Wide-Area Networking Configuration Guide*<br>*Cisco IOS Wide-Area Networking Command Reference* | Frame Relay, Layer 2 Tunneling Protocol Version 3 (L2TPv3), Link Access Procedure, Balanced (LAPB), Switched Multimegabit Data Service (SMDS), and X.25. |
| *Cisco IOS Wireless LAN Configuration Guide*<br>*Cisco IOS Wireless LAN Command Reference* | Broadcast key rotation, IEEE 802.11x support, IEEE 802.1x authenticator, IEEE 802.1x local authentication service for Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Multiple Basic Service Set ID (BSSID), Wi-Fi Multimedia (WMM) required elements, and Wi-Fi Protected Access (WPA). |

*Table 2 Cisco IOS Supplementary Documents and Resources*

| Document Title | Description |
|---|---|
| *Cisco IOS Master Command List, All Releases* | Alphabetical list of all the commands documented in all Cisco IOS releases. |
| *Cisco IOS New, Modified, Removed, and Replaced Commands* | List of all the new, modified, removed, and replaced commands for a Cisco IOS release. |
| *Cisco IOS Software System Messages* | List of Cisco IOS system messages and descriptions. System messages may indicate problems with your system; be informational only; or may help diagnose problems with communications lines, internal hardware, or the system software. |
| *Cisco IOS Debug Command Reference* | Alphabetical list of **debug** commands including brief descriptions of use, command syntax, and usage guidelines. |
| Release Notes and Caveats | Information about new and changed features, system requirements, and other useful information about specific software releases; information about defects in specific Cisco IOS software releases. |
| MIBs | Files used for network monitoring. To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator at the following URL:<br>http://www.cisco.com/go/mibs |
| RFCs | Standards documents maintained by the Internet Engineering Task Force (IETF) that Cisco IOS documentation references where applicable. The full text of referenced RFCs may be obtained at the following URL:<br>http://www.rfc-editor.org/ |

# Additional Resources and Documentation Feedback

*What's New in Cisco Product Documentation* is published monthly and describes all new and revised Cisco technical documentation. The *What's New in Cisco Product Documentation* publication also provides information about obtaining the following resources:

- Technical documentation
- Cisco product security overview
- Product alerts and field notices
- Technical assistance

Cisco IOS technical documentation includes embedded feedback forms where you can rate documents and provide suggestions for improvement. Your feedback helps us improve our documentation.

# Using the Command-Line Interface in Cisco IOS and Cisco IOS XE Software

**Last updated: August 6, 2008**

This document provides basic information about the command-line interface (CLI) in Cisco IOS and Cisco IOS XE software and how you can use some of the CLI features. This document contains the following sections:



For more information about using the CLI, see the "Using the Cisco IOS Command-Line Interface" section of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

For information about the software documentation set, see the "About Cisco IOS and Cisco IOS XE Software Documentation" document.

## Initially Configuring a Device

Initially configuring a device varies by platform. For information about performing an initial configuration, see the hardware installation documentation that is provided with the original packaging of the product or go to the Product Support area of Cisco.com at http://www.cisco.com/web/psa/products/index.html.

After you have performed the initial configuration and connected the device to your network, you can configure the device by using the console port or a remote access method, such as Telnet or Secure Shell (SSH), to access the CLI or by using the configuration method provided on the device, such as Security Device Manager.

### Changing the Default Settings for a Console or AUX Port

There are only two changes that you can make to a console port and an AUX port:

- Change the port speed with the **config-register 0x** command. Changing the port speed is not recommended. The well-known default speed is 9600.
- Change the behavior of the port; for example, by adding a password or changing the timeout value.

**Note** The AUX port on the Route Processor (RP) installed in a Cisco ASR1000 series router does not serve any useful customer purpose and should be accessed only under the advisement of a customer support representative.

# Using the CLI

This section describes the following topics:



## Understanding Command Modes

The CLI command mode structure is hierarchical, and each mode supports a set of specific commands. This section describes the most common of the many modes that exist.

Table 1 lists common command modes with associated CLI prompts, access and exit methods, and a brief description of how each mode is used.

*Table 1 CLI Command Modes*

| Command Mode | Access Method | Prompt | Exit Method | Mode Usage |
|---|---|---|---|---|
| User EXEC | Log in. | `Router>` | Issue the **logout** or **exit** command. | • Change terminal settings.<br>• Perform basic tests.<br>• Display device status. |
| Privileged EXEC | From user EXEC mode, issue the **enable** command. | `Router#` | Issue the **disable** command or the **exit** command to return to user EXEC mode. | • Issue **show** and **debug** commands.<br>• Copy images to the device.<br>• Reload the device.<br>• Manage device configuration files.<br>• Manage device file systems. |
| Global configuration | From privileged EXEC mode, issue the **configure terminal** command. | `Router(config)#` | Issue the **exit** command or the **end** command to return to privileged EXEC mode. | Configure the device. |
| Interface configuration | From global configuration mode, issue the **interface** command. | `Router(config-if)#` | Issue the **exit** command to return to global configuration mode or the **end** command to return to privileged EXEC mode. | Configure individual interfaces. |
| Line configuration | From global configuration mode, issue the **line vty** or **line console** command. | `Router(config-line)#` | Issue the **exit** command to return to global configuration mode or the **end** command to return to privileged EXEC mode. | Configure individual terminal lines. |

*Table 1 CLI Command Modes (continued)*

| Command Mode | Access Method | Prompt | Exit Method | Mode Usage |
|---|---|---|---|---|
| ROM monitor | From privileged EXEC mode, issue the **reload** command. Press the **Break** key during the first 60 seconds while the system is booting. | `rommon # >`<br>The # symbol represents the line number and increments at each prompt. | Issue the **continue** command. | • Run as the default operating mode when a valid image cannot be loaded.<br>• Access the fall-back procedure for loading an image when the device lacks a valid image and cannot be booted.<br>• Perform password recovery when a CTRL-Break sequence is issued within 60 seconds of a power-on or reload event. |
| Diagnostic (available only on the Cisco ASR1000 series router) | The router boots or enters diagnostic mode in the following scenarios. When a Cisco IOS process or processes fail, in most scenarios the router will reload.<br>• A user-configured access policy was configured using the **transport-map** command, which directed the user into diagnostic mode.<br>• The router was accessed using an RP auxiliary port.<br>• A break signal (**Ctrl-C**, **Ctrl-Shift-6**, or the **send break** command) was entered, and the router was configured to enter diagnostic mode when the break signal was received. | `Router(diag)#` | If a Cisco IOS process failure is the reason for entering diagnostic mode, the failure must be resolved and the router must be rebooted to exit diagnostic mode.<br>If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or using a method that is configured to connect to the Cisco IOS CLI.<br>If the RP auxiliary port was used to access the router, use another port for access. Accessing the router through the auxiliary port is not useful for customer purposes. | • Inspect various states on the router, including the Cisco IOS state.<br>• Replace or roll back the configuration.<br>• Provide methods of restarting the Cisco IOS software or other processes.<br>• Reboot hardware, such as the entire router, an RP, an ESP, a SIP, a SPA, or possibly other hardware components.<br>• Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP. |

EXEC commands are not saved when the software reboots. Commands that you issue in a configuration mode can be saved to the startup configuration. If you save the running configuration to the startup configuration, these commands will execute when the software is rebooted. Global configuration mode is the highest level of configuration mode. From global configuration mode, you can enter a variety of other configuration modes, including protocol-specific modes.

ROM monitor mode is a separate mode that is used when the software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode. Use the question symbol (?) to view the commands that you can use while the device is in ROM monitor mode.

```
rommon 1 > ?
alias               set and display aliases command
boot                boot up an external process
confreg             configuration register utility
cont                continue executing a downloaded image
context             display the context of a loaded image
cookie              display contents of cookie PROM in hex
.
.
.
rommon 2 >
```

The following example shows how the command prompt changes to indicate a different command mode:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 1/1
Router(config-if)# ethernet
Router(config-line)# exit
Router(config)# end
Router#
```

**Note** A keyboard alternative to the **end** command is Ctrl-Z.

# Using the Interactive Help Feature

The CLI includes an interactive Help feature. Table 2 describes how to use the Help feature.

***Table 2 CLI Interactive Help Commands***

| Command | Purpose |
|---|---|
| **help** | Provides a brief description of the help feature in any command mode. |
| **?** | Lists all commands available for a particular command mode. |
| *partial command***?** | Provides a list of commands that begin with the character string (no space between the command and the question mark). |
| *partial command*<**Tab**> | Completes a partial command name (no space between the command and <Tab>). |
| *command* **?** | Lists the keywords, arguments, or both associated with the command (space between the command and the question mark). |
| *command keyword* **?** | Lists the arguments that are associated with the keyword (space between the keyword and the question mark). |

The following examples show how to use the help commands:

**help**

```
Router> help

Help may be requested at any point in a command by entering a question mark '?'.  If
nothing matches, the help list will be empty and you must backup until entering a '?'
shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?')
and describes each possible argument.

2. Partial help is provided when an abbreviated argument is entered and you want to know
what arguments match the input (e.g. 'show pr?'.)
```

**?**

```
Router# ?
Exec commands:
  access-enable        Create a temporary access-List entry
  access-profile       Apply user-profile to interface
  access-template      Create a temporary access-List entry
  alps                 ALPS exec commands
  archive              manage archive files
<snip>
```

***partial command*?**

```
Router(config)# zo?
zone  zone-pair
```

***partial command*<Tab>**

```
Router(config)# we<Tab> webvpn
```

***command* ?**

```
Router(config-if)# pppoe ?
  enable        Enable pppoe
  max-sessions  Maximum PPPOE sessions
```

***command keyword* ?**

```
Router(config-if)# pppoe enable ?
  group  attach a BBA group
  <cr>
```

# Understanding Command Syntax

Command syntax is the format in which a command should be entered in the CLI. Commands include the name of the command, keywords, and arguments. Keywords are alphanumeric strings that are used literally. Arguments are placeholders for values that a user must supply. Keywords and arguments may be required or optional.

Specific conventions convey information about syntax and command elements. Table 3 describes these conventions.

*Table 3 CLI Syntax Conventions*

| Symbol/Text | Function | Notes |
|---|---|---|
| < > (angle brackets) | Indicate that the option is an argument. | Sometimes arguments are displayed without angle brackets. |
| A.B.C.D. | Indicates that you must enter a dotted decimal IP address. | Angle brackets (< >) are not always used to indicate that an IP address is an argument. |
| WORD (all capital letters) | Indicates that you must enter one word. | Angle brackets (< >) are not always used to indicate that a WORD is an argument. |
| LINE (all capital letters) | Indicates that you must enter more than one word. | Angle brackets (< >) are not always used to indicate that a LINE is an argument. |
| <cr> (carriage return) | Indicates the end of the list of available keywords and arguments, and also indicates when keywords and arguments are optional. When <cr> is the only option, you have reached the end of the branch or the end of the command if the command has only one branch. | — |

The following examples show syntax conventions:

```
Router(config)# ethernet cfm domain ?
  WORD  domain name
Router(config)# ethernet cfm domain dname ?
  level
Router(config)# ethernet cfm domain dname level ?
  <0-7>  maintenance level number
Router(config)# ethernet cfm domain dname level 7 ?
  <cr>
Router(config)# snmp-server file-transfer access-group 10 ?
  protocol  protocol options
  <cr>
Router(config)# logging host ?
  Hostname or A.B.C.D  IP address of the syslog server
  ipv6                 Configure IPv6 syslog server
Router(config)# snmp-server file-transfer access-group 10 ?
  protocol  protocol options
  <cr>
```

# Understanding Enable and Enable Secret Passwords

Some privileged EXEC commands are used for actions that impact the system, and it is recommended that you set a password for these commands to prevent unauthorized use. Two types of passwords, enable (not encrypted) and enable secret (encrypted), can be set. The following commands set these passwords and are issued in global configuration mode:

- **enable** *password*
- **enable secret** *password*

Using an enable secret password is recommended because it is encrypted and more secure than the enable password. When you use an enable secret password, text is encrypted (unreadable) before it is written to the config.text file. When you use an enable password, the text is written as entered (readable) to the config.text file.

Each type of password is case sensitive, can contain from 1 to 25 uppercase and lowercase alphanumeric characters, and can start with a number. Spaces are also valid password characters; for example, "two words" is a valid password. Leading spaces are ignored, but trailing spaces are recognized.

**Note** Both password commands have numeric keywords that are single integer values. If you choose a number for the first character of your password followed by a space, the system will read the number as if it were the numeric keyword and not as part of your password.

When both passwords are set, the enable secret password takes precedence over the enable password.

To remove a password, use the **no** form of the commands: **no enable** *password* or **no enable secret** *password*.

For more information about password recovery procedures for Cisco products, see http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml.

# Using the Command History Feature

The CLI command history feature saves the commands you enter during a session in a command history buffer. The default number of commands saved is 10, but the number is configurable within the range of 0 to 256. This command history feature is particularly useful for recalling long or complex commands.

To change the number of commands saved in the history buffer for a terminal session, issue the **terminal history size** command:

```
Router# terminal history size num
```

A command history buffer is also available in line configuration mode with the same default and configuration options. To set the command history buffer size for a terminal session in line configuration mode, issue the **history** command:

```
Router(config-line)# history [size num]
```

To recall commands from the history buffer, use the following methods:

- Press Ctrl-P or the up arrow key—Recalls commands beginning with the most recent command. Repeat the key sequence to recall successively older commands.

- Press Ctrl-N or the down arrow key—Recalls the most recent commands in the history buffer after they have been recalled using Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.

**Note** The arrow keys function only on ANSI-compatible terminals such as the VT100.

- Issue the **show history** command in user EXEC or privileged EXEC mode—Lists the most recent commands that you entered. The number of commands that are displayed is determined by the setting of the **terminal history size** and **history** commands.

  The CLI command history feature is enabled by default. To disable this feature for a terminal session, issue the **terminal no history** command in user EXEC or privileged EXEC mode or the **no history** command in line configuration mode.

# Abbreviating Commands

Typing a complete command name is not always required for the command to execute. The CLI recognizes an abbreviated command when the abbreviation contains enough characters to uniquely identify the command. For example, the **show version** command can be abbreviated as **sh ver**. It cannot be abbreviated as **s ver** because **s** could mean **show**, **set**, or **systat**. The **sh v** abbreviation also is not valid because the **show** command has **vrrp** as a keyword in addition to **version**. (Command and keyword examples from Cisco IOS Release 12.4(13)T.)

# Using Aliases for CLI Commands

To save time and the repetition of entering the same command multiple times, you can use a command alias. An alias can be configured to do anything that can be done at the command line, but an alias cannot move between modes, type in passwords, or perform any interactive functions.

Table 4 shows the default command aliases.

***Table 4 Default Command Aliases***

| Command Alias | Original Command |
|---|---|
| **h** | help |
| **lo** | logout |
| **p** | ping |
| **s** | show |
| **u** or **un** | undebug |
| **w** | where |

To create a command alias, issue the **alias** command in global configuration mode. The syntax of the command is **alias** *mode command-alias original-command*. Following are some examples:

- Router(config)# **alias exec prt partition**—privileged EXEC mode
- Router(config)# **alias configure sb source-bridge**—global configuration mode
- Router(config)# **alias interface rl rate-limit**—interface configuration mode

To view both default and user-created aliases, issue the **show alias** command.

For more information about the **alias** command, see http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html.

# Using the no and default Forms of Commands

Most configuration commands have a **no** form that is used to reset a command to its default value or disable a feature or function. For example, the **ip routing** command is enabled by default. To disable this command, you would issue the **no ip routing** command. To re-enable IP routing, you would issue the **ip routing** command.

Configuration commands may also have a **default** form, which returns the command settings to their default values. For commands that are disabled by default, using the **default** form has the same effect as using the **no** form of the command. For commands that are enabled by default and have default settings, the **default** form enables the command and returns the settings to their default values.

The **no** and **default** forms of commands are described in the command pages of command references.

# Using the debug Command

A **debug** command produces extensive output that helps you troubleshoot problems in your network. These commands are available for many features and functions within Cisco IOS and Cisco IOS XE software. Some **debug** commands are **debug all**, **debug aaa accounting**, and **debug mpls packets**. To use **debug** commands during a Telnet session with a device, you must first enter the **terminal monitor** command. To turn off debugging completely, you must enter the **undebug all** command.

For more information about **debug** commands, see the *Cisco IOS Debug Command Reference* at http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html.

**Caution** Debugging is a high priority and high CPU utilization process that can render your device unusable. Use **debug** commands only to troubleshoot specific problems. The best times to run debugging are during periods of low network traffic and when few users are interacting with the network. Debugging during these periods decreases the likelihood that the **debug** command processing overhead will affect network performance or user access or response times.

# Filtering Output Using Output Modifiers

Many commands produce lengthy output that may use several screens to display. Using output modifiers, you can filter this output to show only the information that you want to see.

Three output modifiers are available and are described as follows:

- **begin** *regular expression*—Displays the first line in which a match of the regular expression is found and all lines that follow.
- **include** *regular expression*—Displays all lines in which a match of the regular expression is found.
- **exclude** *regular expression*—Displays all lines except those in which a match of the regular expression is found.

To use one of these output modifiers, type the command followed by the pipe symbol (|), the modifier, and the regular expression that you want to search for or filter. A regular expression is a case-sensitive alphanumeric pattern. It can be a single character or number, a phrase, or a more complex string.

The following example illustrates how to filter output of the **show interface** command to display only lines that include the expression "protocol."

```
Router# show interface | include protocol

FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

# Understanding CLI Error Messages

You may encounter some error messages while using the CLI. Table 5 shows the common CLI error messages.

***Table 5 Common CLI Error Messages***

| Error Message | Meaning | How to Get Help |
|---|---|---|
| % Ambiguous command: "show con" | You did not enter enough characters for the command to be recognized. | Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear. |
| % Incomplete command. | You did not enter all the keywords or values required by the command. | Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear. |
| % Invalid input detected at "^" marker. | You entered the command incorrectly. The caret (^) marks the point of the error. | Enter a question mark (?) to display all the commands that are available in this command mode. The keywords that you are allowed to enter for the command appear. |

For more system error messages, see the following documents:

- *Cisco IOS Release 12.2SR System Message Guide*
- *Cisco IOS System Messages, Volume 1 of 2* (Cisco IOS Release 12.4)
- *Cisco IOS System Messages, Volume 2 of 2* (Cisco IOS Release 12.4)

# Saving Changes to a Configuration

To save changes that you made to the configuration of a device, you must issue the **copy running-config startup-config** command or the **copy system:running-config nvram:startup-config** command. When you issue these commands, the configuration changes that you made are saved to the startup configuration and saved when the software reloads or power to the device is turned off or interrupted. The following example shows the syntax of the **copy running-config startup-config** command:

```
Router# copy running-config startup-config
Destination filename [startup-config]?
```

You press Enter to accept the startup-config filename (the default), or type a new filename and then press Enter to accept that name. The following output is displayed indicating that the configuration was saved:

```
Building configuration...
[OK]
Router#
```

On most platforms, the configuration is saved to NVRAM. On platforms with a Class A flash file system, the configuration is saved to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM.

# Additional Information

- "Using the Cisco IOS Command-Line Interface" section of the *Cisco IOS Configuration Fundamentals Configuration Guide*:

  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html

  or

  "Using Cisco IOS XE Software" chapter of the *Cisco ASR1000 Series Aggregation Services Routers Software Configuration Guide*:

  http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/using_cli.html
- Cisco Product Support Resources

  http://www.cisco.com/web/psa/products/index.html
- Support area on Cisco.com (also search for documentation by task or product)

  http://www.cisco.com/en/US/support/index.html
- *White Paper: Cisco IOS Reference Guide*

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_white_paper09186a008018305e.shtml
- Software Download Center (downloads; tools; licensing, registration, advisory, and general information) (requires Cisco.com User ID and password)

  http://www.cisco.com/kobayashi/sw-center/
- Error Message Decoder, a tool to help you research and resolve error messages for Cisco IOS software

  http://www.cisco.com/pcgi-bin/Support/Errordecoder/index.cgi

- Command Lookup Tool, a tool to help you find detailed descriptions of Cisco IOS commands (requires Cisco.com user ID and password)

  http://tools.cisco.com/Support/CLILookup

- Output Interpreter, a troubleshooting tool that analyzes command output of supported **show** commands

  https://www.cisco.com/pcgi-bin/Support/OutputInterpreter/home.pl\

---

CHAPTER 1

# Overview of the Cisco Mobile Wireless Home Agent

This chapter illustrates the functional elements in a typical CDMA2000 packet data system, the Cisco products that are currently available to support this solution. and their implementation in Cisco IOS Mobile Wireless Home Agent software.

This chapter includes the following sections:



## Feature Overview

Cisco's Mobile Wireless Packet Data Solution includes the Packet Data Serving Node (PDSN) with Foreign Agent (FA) functionality, the Cisco Mobile Wireless Home Agent (HA), Authentication, Authorization and Accounting (AAA) servers, and several other security products and features. The solution is standards compliant, and is designed to meet the needs of the mobile wireless industry as it transitions towards third-generation cellular data services.

The Home Agent is the anchor point for mobile terminals for which MobileIP or Proxy MobileIP services are provided. Traffic sent to the terminal is routed through the Home Agent. With reverse tunneling, traffic from the terminal is also routed through the Home Agent.

A PDSN provides access to the Internet, intranets, and Wireless Application Protocol (WAP) servers for mobile stations using a Code Division Multiple Access 2000 (CDMA2000) Radio Access Network (RAN). The Cisco PDSN is a Cisco IOS software feature that runs on Cisco 7200 routers, Catalyst 6500 switches, and Cisco 7600 Internet routers, and acts as an access gateway for Simple IP and Mobile IP stations. It provides FA support and packet transport for virtual private networking (VPN). It also acts as a AAA client.

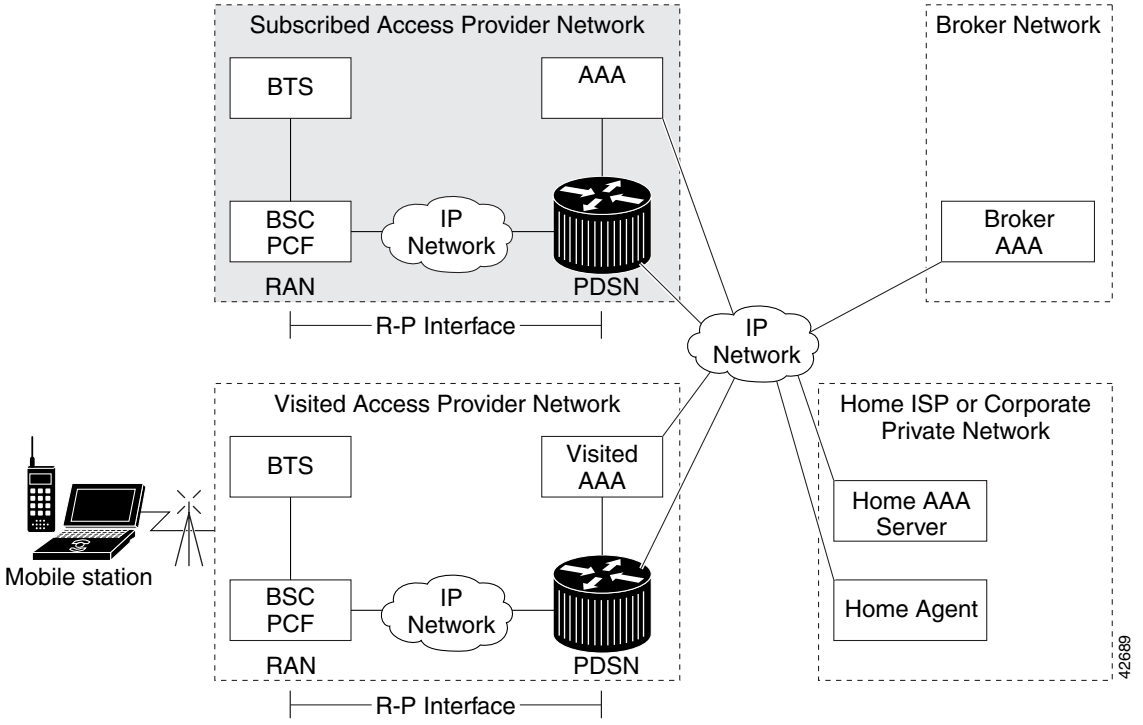
The Cisco PDSN and the Cisco Home Agent support all relevant 3GPP2 standards, including those that define the overall structure of a CDMA2000 network, and the interfaces between radio components, the Home Agent, and the PDSN.

# System Overview

CDMA is one of the standards for mobile communication. A typical CDMA2000 network includes terminal equipment, mobile termination, base transceiver stations (BTSs), base station controllers (BSCs), PDSNs, and other CDMA network and data network entities. The PDSN is the interface between a BSC and a network router.

Figure 1-1 illustrates the relationship of the components of a typical CDMA2000 network, including a PDSN and a Home Agent. In this illustration, a roaming mobile station user is receiving data services from a visited access provider network, rather than from the mobile station user's subscribed access provider network.

***Figure 1-1 The CDMA Network***




As the illustration shows, the mobile station, which must support either Simple IP or Mobile IP, connects to a radio tower and BTS. The BTS connects to a BSC, which contains a component called the Packet Control Function (PCF). The PCF communicates with the Cisco PDSN through an A10/A11 interface. The A10 interface is for user data and the A11 interface is for control messages. This interface is also known as the RAN-to-PDSN (R-P) interface. For the Cisco Home Agent Release 2.1 and above, you must use a Fast Ethernet (FE) interface as the R-P interface on the Cisco 7200 platform, and a Giga Ethernet (GE) interface on the Cisco Multi-Processor WAN Application Module (MWAM) platform.

The IP networking between the PDSN and external data networks is through the PDSN-to-intranet/Internet ($P_i$) interface. For the Cisco Home Agent, you can use either an FE or GE interface as the $P_i$ interface.

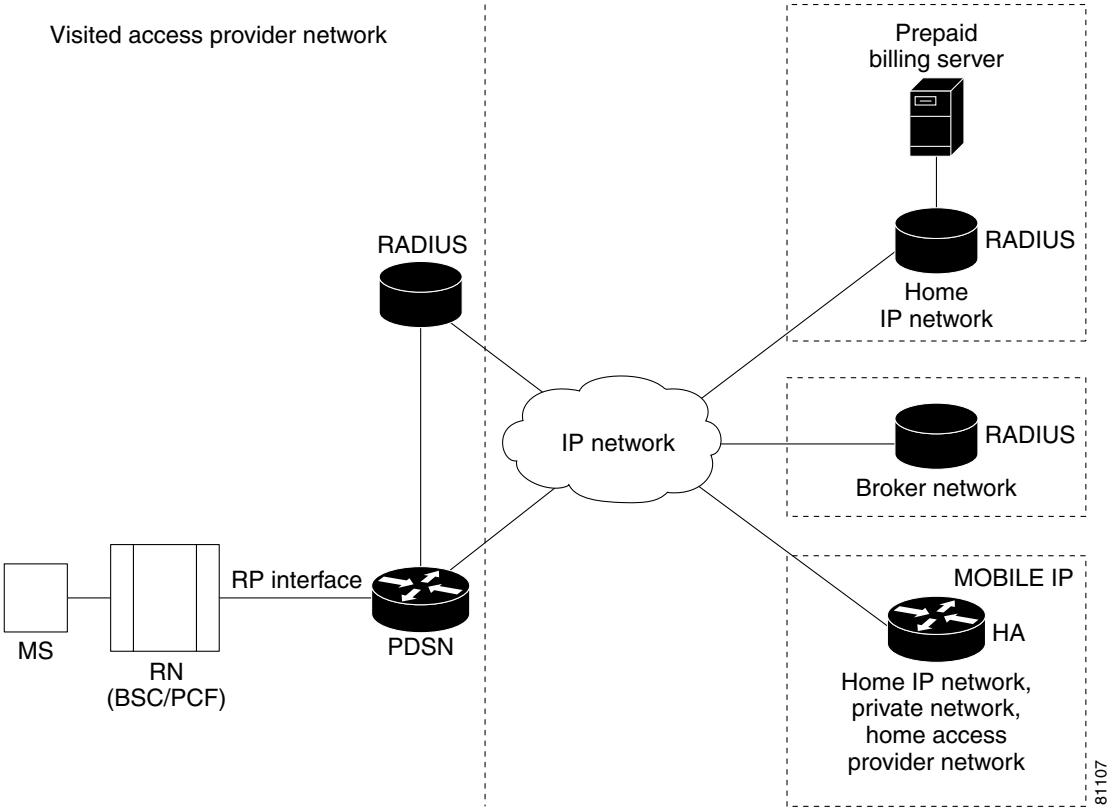
For "back office" connectivity, such as connections to a AAA server, the interface is media independent. Any of the interfaces supported on the Cisco 7206 can be used to connect to these types of services, but we recommend that you use either an FE or GE interface as the $P_i$ interface.

# Cisco Home Agent Network

Figure 1-2 illustrates the functional elements in a typical CDMA2000 packet data system, and Cisco products that are currently available to support this solution. The Home Agent, in conjunction with the PDSN and Foreign Agent, allows a mobile station with Mobile IP client function, to access the Internet or corporate intranet using Mobile IP-based service access. Mobile IP extends user mobility beyond the coverage area of the current, serving PDSN/Foreign Agent. If another PDSN is allocated to the call (following a handoff), the target PDSN performs a Mobile IP registration with the Home Agent; this ensures that the same home address is allocated to the mobile station. Additionally, clients without a Mobile IP client can also make use of these services by using the Proxy Mobile IP capability provided by the PDSN.

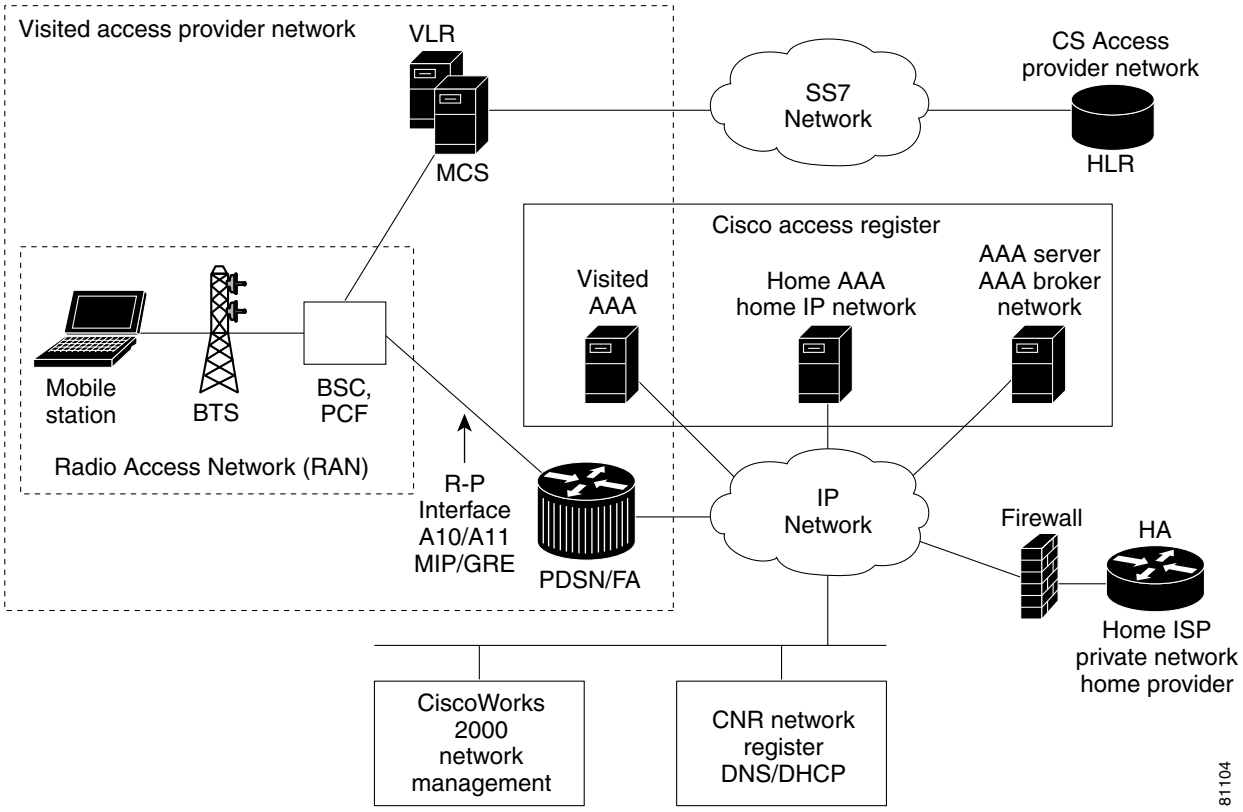
The Home Agent, then, is the anchor point for mobile terminals for which Mobile IP or Proxy Mobile IP services are provided. Traffic is routed through the Home Agent, and the Home Agent also provides Proxy ARP services. In the case of reverse tunneling, traffic from the terminal is also routed through the Home Agent.

***Figure 1-2 Cisco Products for CDMA2000 Packet Data Services Solution***




For Mobile IP services, the Home Agent would typically be located within an ISP network, or within a corporate domain. However, many ISPs and/or corporate entities may not be ready to provision Home Agents by the time service providers begin rollout of third-generation packet data services. As a remedy, Access service providers could provision Home Agents within their own domains, and then forward packets to ISPs or corporate domains using VPDN services. Figure 1-3 illustrates the functional elements that are necessary to support Mobile IP-based service access when the Home Agent is located in the service provider domain.

*Figure 1-3 Cisco Mobile IP-Based Service Access With Home Agent in Service Provider Network*




For Mobile IP and Proxy-Mobile IP types of access, these solutions allow a mobile user to roam within and beyond its service provider boundaries, while always being reachable and addressable through the IP address assigned on initial session establishment. Details of Mobile IP and Proxy Mobile IP Services can be found in the Packet Data Services section that follows.

# Packet Data Services

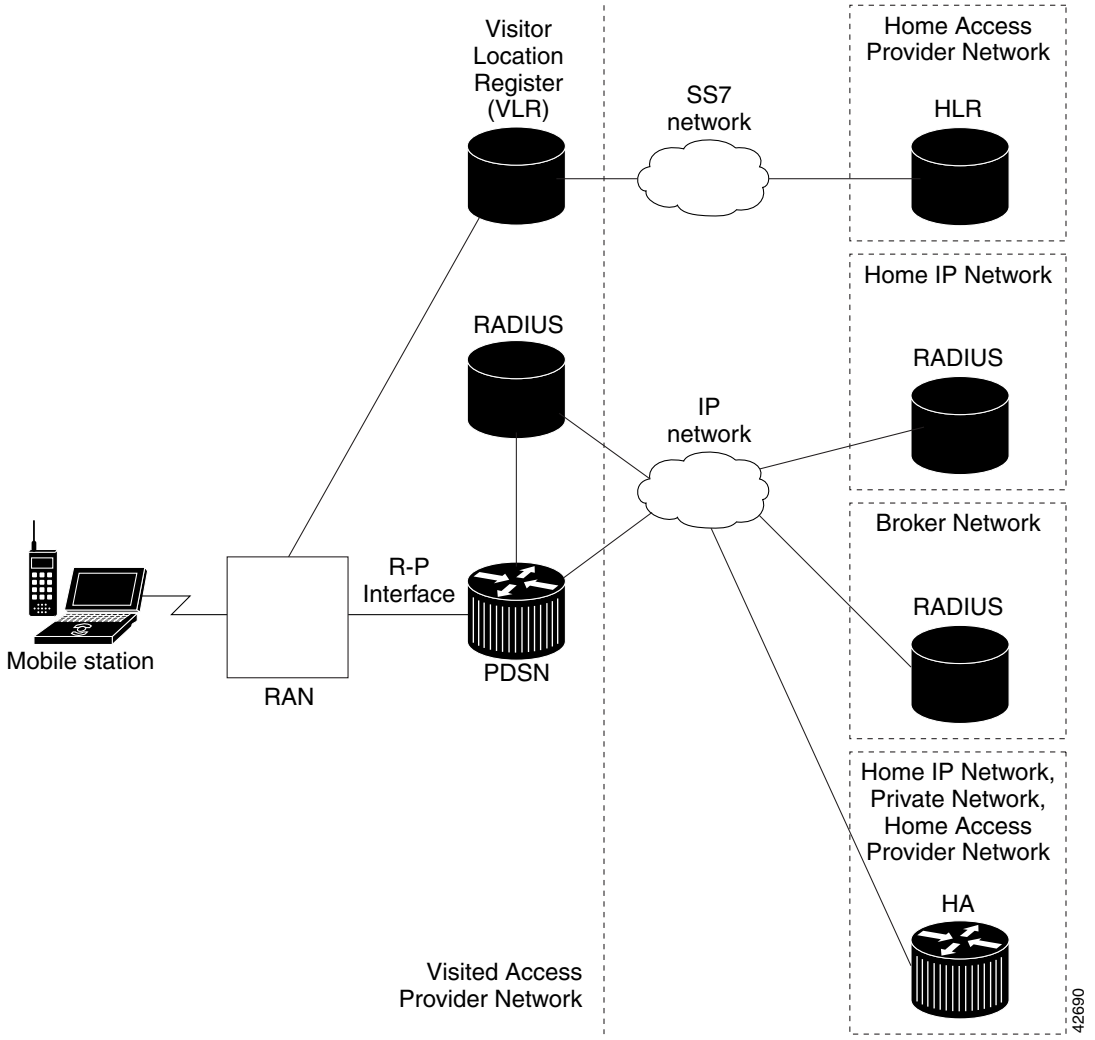
In the context of a CDMA2000 network, the Cisco Home Agent supports two types of packet data services: Mobile IP and Proxy Mobile IP services. From the perspective of the Cisco Home Agent, these services are identical.

## Cisco Mobile IP Service

With Mobile IP, the mobile station can roam beyond the coverage area of a given PDSN and still maintain the same IP address and application-level connections.

Figure 1-4 shows the placement of the Cisco Home Agent in a Mobile IP scenario.

*Figure 1-4 CDMA Network—Mobile IP Scenario*




The communication process occurs in the following order:

1. The mobile station registers with its Home Agent (HA) through an FA. In the context of the CDMA2000 network, the FA is the Cisco PDSN.
2. The Cisco HA accepts the registration, assigns an IP address to the mobile station, and creates a tunnel to the FA. The resulting configuration is a PPP link between the mobile station and the FA (or PDSN), and an IP-in-IP or GRE tunnel between the FA and the HA.

   As part of the registration process, the Cisco HA creates a binding table entry to associate the mobile station's home address with its *Care-of* Address (CoA).

**Note** While away from home (from the HA's perspective), the mobile station is associated with a care-of address. This address identifies the mobile station's current, topological point of attachment to the Internet, and is used to route packets to the mobile station. Either a Foreign Agent's address, or an address obtained by the mobile station for use while it is present on a particular network, is used as the care-of address. In the case of the Cisco Home Agent, the care-of address is always an address of the Foreign Agent.

3. The HA advertises network reachability to the mobile station, and tunnels datagrams to the mobile station at its current location.
4. The mobile station sends packets with its home address as the source IP address.
5. Packets destined for the mobile station go through the HA, which tunnels them to the PDSN. From there they are sent to the mobile station using the care-of address. This scenario also applies to reverse tunneling, which allows traffic moving from the mobile to the network to pass through the Home Agent.
6. When the PPP link is handed off to a new PDSN, the link is renegotiated and the Mobile IP registration is renewed.
7. The HA updates its binding table with the new care-of address.

**Note** For more information about Mobile IP, refer to the Cisco IOS Release 12.3 documentation modules *Cisco IOS IP Configuration Guide* and *Cisco IOS IP Command Reference.* RFC 2002 describes the specification in detail. TIA/EIA/IS-835-B also defines how Mobile IP is realized in the Home Agent.

# Cisco Proxy Mobile IP Service

While PPP, which is widely used to connect to an Internet Service Provider (ISP), is ubiquitous in IP devices, certain service providers lack commercially available Mobile IP client software. As an alternative to Mobile IP, you can use Cisco's Proxy Mobile IP feature. This capability of the Cisco PDSN, which is integrated with PPP, enables the PDSN (functioning as a Foreign Agent) and a Mobile IP client, to provide mobility to authenticated PPP users.

The communication process occurs in the following order:

1. The Cisco PDSN (acting as an FA) collects and sends mobile station authentication information to the AAA server (specifically, PPP authentication information).
2. If the mobile station is successfully authorized to use Cisco PDSN Proxy Mobile IP service, the AAA server returns the registration data and an HA address.
3. The FA uses this information, and other data, to generate a registration request (RRQ) on behalf of the mobile station, and sends it to the Cisco HA.
4. If the registration is successful, the Cisco HA sends a registration reply (RRP) that contains an IP address to the FA.
5. The FA assigns the IP address (received in the RRP) to the mobile station, using IP control protocol (IPCP).
6. A tunnel is established between the Cisco HA and the FA, or PDSN. If reverse tunneling is enabled, the tunnel carries traffic to and from the mobile station.

**Note** The PDSN takes care of all Mobile IP re-registrations on behalf of the Proxy-MIP client.

# Features

## New Features in IOS Release 12.3(14)YX1

This section lists features that were introduced or modified in Home Agent Release 12.3(14)YX1:

- Mobile Equipment Identifier (MEID) Support

This section describes features that were introduced or modified in Home Agent Release 3.0:

- Home Agent Accounting Enhancements
  - Home Agent Accounting in a Redundant Setup
  - Packet count and Byte count in Accounting Records
  - Additional Attributes in the Accounting Records
  - Additional Accounting Methods—Interim Accounting is Supported.
- VRF Mapping on the RADIUS Server
- Conditional Debugging Enhancements
- Home Agent Redundancy Enhancements
  - Geographical Redundancy
  - Redundancy with Radius Downloaded Pool Names
- SNMP Traps to Track Utilization of Local IP Pool
- Support for Supervisor 720 and 1GB MWAM in Supported Platforms
- Mobile-User ACLs in Packet Filtering
- IP Reachability
- DNS Server Address Assignment
- Mobile IP MIB Enhancements in SNMP, MIBs and Network Management

This section lists features that were introduced or modified in previous releases of the Cisco Mobile Wireless Home Agent:

- Mobile IPv4 Registration Revocation, page 7-1
- HA Server Load Balancing, page 6-1
- Home Agent Accounting, page 11-1
- Skip HA-CHAP with MN-FA Challenge Extension (MFCE), page 4-2
- VRF Support on HA, page 12-1
- Hot-lining, page 13-1
- Radius Disconnect, page 7-4
- Conditional Debugging, page 15-3
- Home Address Assignment, page 3-1
- Home Agent Redundancy, page 5-1
- Virtual Networks, page 5-6
- On-Demand Address Pool (ODAP), page 3-6

- Mobile IP IPSec, page 10-2
- Support for ACLs on Tunnel Interface, page 14-1
- Support for AAA Attributes MN-HA-SPI and MN-HA SHARED KEY, page 14-3
- 3 DES Encryption, page 10-1
- User Profiles, page 14-3
- Mobility Binding Association, page 14-4
- User Authentication and Authorization, page 4-1
- HA Binding Update, page 14-4
- Per User Packet Filtering, page 9-1
- Security, page 10-1

## Feature Support

In addition to supporting Cisco IOS networking features, a Cisco 7200 series router, Cisco 6500 series switch, or Cisco 7600 series router, configured as a Home Agent, supports the following Home Agent-specific features:

- Support for static IP addresses assignment
  - Public IP addresses
  - Private IP addresses
- Support for dynamic IP addresses assignment
  - Public IP addresses
  - Private IP addresses
- Multiple flows for different Network Access Identifiers (NAIs) using static or dynamic addresses
- Multiple flows for the same NAI using different static addresses
- Foreign Agent Challenge extensions in RFC 3012 - bis 03
  - Mobile IP Agent Advertisement Challenge Extension
  - MN-FA Challenge Extension
  - Generalized Mobile IP Authentication Extension, which specifies the format for the MN-AAA Authentication Extension
- Mobile IP Extensions specified in RFC 2002
  - MN-HA Authentication Extension
  - FA-HA Authentication Extension
- Reverse Tunneling, RFC 2344
- Mobile NAI Extension, RFC 2794
- Multiple tunneling modes between FA and HA
  - IP-in-IP Encapsulation, RFC 2003
  - Generic Route Encapsulation, RFC 2784
- Binding Update message for managing stale bindings
- Home Agent redundancy support

- Mobile IP Extensions specified in RFC 3220
  - Authentication requiring the use of SPI. section 3.2
- Support for Packet Filtering
  - Input access lists
  - Output access lists
- Support for proxy and gratuitous ARP
- Mobile IP registration replay protection using time stamps. Nonce-based replay protection is not supported.

## Benefits

The Cisco Mobile Wireless Home Agent provides these additional benefits:

- Supports static and dynamic IP address allocation.
- Attracts, intercepts, and tunnels datagrams for delivery to the MS.
- Receives tunneled datagrams from the MS (through the FA), unencapsulates them, and delivers them to the corresponding node (CN).

**Note** Depending on the configuration, reverse tunneling may, or may not, be used by the MS, and may or may not be accepted by the HA.

- Presents a unique routable address to the network.
- Supports ingress and egress filtering.
- Maintains binding information for each registered MS containing an association of Care-of Address (CoA) with the home address, NAI, and security keys together with the lifetime of that association.
- Receives and processes registration renewal requests within the bounds of the Mobile IP registration lifetime timer, either from the MS (through the FA in the Mobile IP case), or from the FA (in the Proxy Mobile IP case).
- Receives and processes de-registration requests either from the MS (through the FA in the Mobile IP case), or from the FA (in the Proxy Mobile IP case).
- Maintains a subscriber database that is stored locally or retrieved from an external source.
- Sends a binding update to the source PDSN under hand-off conditions when suitably configured.
- Supports dynamic HA assignment.

# The Home Agent

The Home Agent (HA) maintains mobile user registrations and tunnels packets destined for the mobile to the PDSN/FA. It supports reverse tunneling, and can securely tunnel packets to the PDSN using IPSec. Broadcast packets are not tunneled. Additionally, the HA performs dynamic home address assignment for the mobile. Home address assignment can be from address pools configured locally, through either DHCP server access, or from the AAA server.

The Cisco HA supports proxy Mobile IP functionality, and is available on the Cisco 7600 series router, Cisco 7200 series router, and Cisco 6500 series switch platforms. A Cisco HA based on the Cisco 7200 series router supports up to 262,000 mobile bindings, can process 100 bindings per second, and is RFC 2002, RFC 2003, RFC 2005 and RFC2006 compliant.

A Cisco HA based on the Cisco 7600 series router or Cisco Catalyst 6500 switch, with two MWAM cards housing five active HA images and five standby images, would support the above figures multiplied by 5.

For more information on Mobile IP as it relates to Home Agent configuration tasks, please refer to the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/mobileip.htm.

CHAPTER 1

# Planning to Configure the Home Agent

This chapter provides information that you should know before configuring a Cisco Mobile Wireless Home Agent.

This chapter includes the following sections:



## Supported Platforms

The Cisco HA is available on Cisco's 7206VXR NPE-400 router, 7206VXR NPE-G1 router, 6500 series switch and 7600 series router. The HA supports Fast Ethernet and Gigabit Ethernet interfaces on these platforms.

**Note** Cisco Mobile Wireless Release 3.0, Cisco IOS Release 12.3(14)YX and later, supports both the standard MWAM 512 MB per processor memory option, and the 1 GB per processor memory option.

## Prerequisites

Depending on the platform on which you are implementing a Home Agent, the prerequisites vary. The sections below provide general guidelines to follow before configuring a Cisco Mobile Wireless Home Agent in your network:

# Cisco 7200 Series Platform Prerequisites

Ensure that you meet the following hardware and software requirements before you implement a Home Agent in your network on the Cisco 7200 series router platform.

## Home Agent on the Cisco 7206VXR NPE-400

For platform details and complete list of interfaces supported on 7206VXR NPE-400, please refer to the following URL on Cisco.com:
http://www.cisco.com/en/US/products/hw/routers/ps341/products_installation_guide_book09186a008007daa6.html

The supported configuration on a Cisco 7206VXR with NPE-400 processor is with 512MB DRAM and one PA-2FE-TX FE port adopter, or two PA-FE-TX port adaptors. PA-2FE-TX port adaptor has two 10/100 based Ethernet ports. PA-FE-TX port adapter has one 10/100 based Ethernet port. The I/O controller on the NPE-400 processor supports two more 10/100 based Ethernet ports. Because the PA-FE-TX is end-of-sale, new configurations require the PA-2FE-TX port adaptor.

For IPSec support, a service adaptor (SA-ISA or SA-VAM2) is required. Because SA-ISA is end-of-sale, new configurations utilizing IPSec will require the NPE-G1 with SA-VAM2.

## Home Agent on 7206VXR NPE-G1

For platform details and complete list of interfaces supported on 7206VXR NPE-G1, please refer to the following URL on Cisco.com:
http://www.cisco.com/en/US/products/hw/routers/ps341/products_installation_guide_chapter09186a0080201e63.html

The supported configuration on a Cisco 7206VXR NPE-G1 processor is with 1GB DRAM and one PA-2FE-TX FE port adaptor. The Cisco 7206VXR NPE-G1 has three 10/100/1000 based Ethernet Ports.

For IPSec support, a service adaptor SA-ISA or SA-VAM2 is required. Because the SA-ISA is end-of-sale, new configurations utilizing IPSec will require use of SA-VAM2

# Catalyst 6500 / Cisco 7600 Series Platform Prerequisites

## Home Agent on 6500 Series Switch

For platform details and a complete list of interfaces supported on the Cisco 6500 series switch, please refer to the on-line product information at the following url:
http://www.cisco.com/en/US/products/hw/switches/ps708/index.html

The supported configuration for the HA based on the 6500 Series switch is dependent on the desired capacity, interface type to be deployed, and whether IPSec support is required.

Either a Supervisor Engine 2 with Multilayer Switch Feature Card 2 (MSFC2) and Policy Feature Card 2 (PFC2) is required, or a Supervisor Engine 720 with Multilayer Switch Feature Card 3 (MSFC3) and Policy Feature Card 3BXL (PFC3BXL) is required.

A 1GB MWAM or 512MB MWAM is required to run HA functionality. Each MWAM module supports up to 5 HA images (5 HA instances).

For IPSec support, an IPSec VPN Services Module (VPNSM) is required for each Cisco 6500 series switch chassis.

### Home Agent on 7600 Series Router

For platform details and a complete list of interfaces supported on the Cisco 7600 series router, please refer to the following URL on Cisco.com:
http://www.cisco.com/en/US/products/hw/routers/ps368/index.html

The supported configuration for the HA based on the Cisco 7600 Series switch is dependent on the desired capacity, interface type to be deployed, and whether IPSec support is required.

Either a Supervisor Engine 2 with Multilayer Switch Feature Card 2 (MSFC2) and Policy Feature Card 2 (PFC2) is required, or a Supervisor Engine 720 with Multilayer Switch Feature Card 3 (MSFC3) and Policy Feature Card 3BXL (PFC3BXL) is required.

A 1GB MWAM or 512MB MWAM module is required to run HA functionality. Each MWAM module supports 5 HA images (5 HA instances).

For IPSec support, an IPSec VPN Services Module (VPNSM) is required for each Cisco 7600 series switch chassis.

# Configuration Tasks

The Cisco Home Agent software includes three images, one for the Cisco 7200 Series Router, one for the 7300 Series router, and one for the Cisco Catalyst 6500 switch and Cisco 7600 Series router platforms. This section describes the steps for configuring the Cisco Home Agent. Each image is described by platform number.

- c7200-h1is-mz HA image
- c7301-is-mz HA image
- svcmwam-h1is-mz HA image

## Upgrading a Home Agent Image

To upgrade an image, you will need a compact flash card that has the MP partition from the current image or later, and a recent supervisor image. To locate the images, please go to the Software Center at Cisco.com (http://www.cisco.com/public/sw-center/).

To perform the upgrade perform the following procedure:

**Step 1** Log onto the supervisor and boot the MP partition on the PC.

```
 router #hw-module module 3 reset cf:1
Device BOOT variable for reset = cf:1 Warning:  Device list is not verified.
 >
 > Proceed with reload of module? [confirm] % reset issued for module 3
 >router#
```

**Step 2** Once the module is online, issue the following command:

**copy tftp**: *tftp file location* pclc# *linecard #*-fs:

The upgrade file uses a special format that makes this process slow. The following example illustrates the upgrade process output:

```
router #copy tftp://172.31.219.33/images/c6svcmwam-c6is-mz.bin pclc#3-fs:
  Destination filename [c6svcmwam-c6is-mz.bin]?
  Accessing tftp://172.31.219.33/images/c6svcmwam-c6is-mz.bin...
  Loading images/c6svcmwam-c6is-mz.bin from 10.102.16.25 (via Vlan1):
  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  [OK - 29048727/58096640 bytes]

  29048727 bytes copied in 1230.204 secs (23616 bytes/sec)
router #
  2d21h: %SVCLC-SP-5-STRRECVD: mod 3: <Application upgrade has started>
  2d21h: %SVCLC-SP-5-STRRECVD: mod 3: <Do not reset the module till upgrade completes!!>
  router #

  2d21h: %SVCLC-SP-5-STRRECVD: mod 3: <Application upgrade has succeeded>
  2d21h: %SVCLC-SP-5-STRRECVD: mod 3: <You can now reset the module
```

**Step 3** Boot the MWAM card back to partition 4, and you have an upgraded image.

```
router#hw-module module 3 reset
```

## Upgrading the HA Image From XW-based Image to YX-based Image

If you are upgrading the Home Agent from a XW-based image to a 12.3(14)YX, or 12.4(11)T image, you first need to upgrade the SUP image from a SXB-based image to a SXE-based image.

**Note** We recommend that you upgrade to the Cisco IOS Supervisor Engine 720, Release 12.2(18)SXE3. For more information on the 12.2(18)SXE3 Supervisor image, please refer to the following URL: http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_note09186a00801c8339.html

After you upgrade the SUP image, you can then upgrade the HA image.

### Upgrading the Supervisor Image

To upgrade the Supervisor image, perform the following procedure:

**Step 1** Copy the SUP image to the disks (disk0: / slavedisk0:).

**Step 2** Add the following command to the running config **boot system disk0**: *SUP image name*". Here is an example:

```
boot system disk0:c6k222-pk9sv-mz.122-18.SXD2.bin
```

**Note** This step may require you to unconfigure previously configured instances of this CLI in order to enable the image to properly reload.

**Step 3** Perform a "write memory" so that running configuration is saved on both active and standby SUP.

**Step 4** Issue **reload** command on the active SUP.

**Step 5** Both active and standby supervisors will reload simultaneously and come up with the SXD-based image.

**Note** Issuing the **reload command** on the active SUP will cause both the active and standby Supervisors to reload simultaneously, thus causing some downtime during the upgrade process.

## Upgrading the HA Image on MWAM

To upgrade to the YF-based image on the MWAM, perform the following procedure:

**Step 1** Bring down the active HA by issuing the **hw-module module** *slot #* **reset cf:1** command. The standby HA will take over as the active HA. Log onto the supervisor and boot the MP partition on the PC.

```
router #hw-module module 3 reset cf:1
Device BOOT variable for reset = cf:1 Warning: Device list is not verified.
>

> Proceed with reload of module? [confirm] % reset issued for module 3
>router#
```

**Step 2** Once the module is online, copy the YF image to pclc# *slot* file system by issuing the following command:

**copy tftp:** *tftp file location* **pclc#** *linecard #***-fs**:

The upgrade file uses a special format that makes this process slow. The following example illustrates the upgrade process output:

```
router #copy tftp://198.133.219.33/images/c6svcmwam-c6is-mz.bin pclc#3-fs:
  Destination filename [c6svcmwam-c6is-mz.bin]?
  Accessing tftp://198.133.219.33/images/c6svcmwam-c6is-mz.bin...
  Loading images/c6svcmwam-c6is-mz.bin from 64.102.16.25 (via Vlan1):
  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  [OK - 29048727/58096640 bytes]
  29048727 bytes copied in 1230.204 secs (23616 bytes/sec)
router #
  2d21h: %SVCLC-SP-5-STRRECVD: mod 3: <Application upgrade has started>
  2d21h: %SVCLC-SP-5-STRRECVD: mod 3: <Do not reset the module till upgrade completes!!>
  router #
  2d21h: %SVCLC-SP-5-STRRECVD: mod 3: <Application upgrade has succeeded>
  2d21h: %SVCLC-SP-5-STRRECVD: mod 3: <You can now reset the module
```

**Step 3** Boot the MWAM card back to partition 4, and you have an upgraded image.

```
router#hw-module module 3 reset cf:4
```

**Step 4** Verify that all the bindings opened with the active HA have synced with the processor with new image.

**Step 5** Bring down the active HA with the XW-based image. The newly loaded YF-based HA will now become active.

**Step 6** Perform steps 1 through 3 as described above.

**Note** The downgrade process is similar to the upgrade process; the SUP image should be downgraded first, followed by the HA image.

**Note** For SXD-based SUP images, if **config-on-SUP** mode is used on the MWAM, the startup configuration is written on both the SUP and local file system. This will assist you in upgrading or downgrading the images without losing the HA configuration between XW and YF images.

**Note** The downgraded image always starts with **config-local** due to incompatibility, and so it must be explicitly configured again using **config-on-sup** on every downgrade. Additionally, any further upgrades will start with the mode used by the same version the image used earlier, followed by the mode used by the old version.

### Changing Configuration on Home Agent in a Live Network

If you need to change the working configuration on a Home Agent in a live network environment, perform the following procedure:

**Step 1** Bring the standby HA out of service. An example would be to shut down the HSRP interface towards active HA.

**Step 2** Make the necessary configuration changes on the standby HA, and save the configuration.

**Step 3** Issue the **reload command to bring** the standby HA back into service.

**Step 4** Bring the active HA out of service by shutting down HSRP interface. This will cause the standby to takeover as the active HA.

**Step 5** Make the necessary configuration changes on the active HA, and save the configuration.

**Step 6** Issue the **reload command to bring the active** HA back into service.

**Note** Some outage might occur concerning existing calls on the active HA being cleared forcibly.

**Note** For HA redundancy to work properly, configure the active and standby the same.

## Loading the IOS Image to MWAM

The image download process automatically loads an IOS image onto the three processor complexes on the MWAM. All three complexes on the card run the same version of IOS, so they share the same image source. The software for MWAM bundles the images it needs in flash memory on the PC complex. For more information, refer to the *Cisco Multi-processor WAN Application Module Installation and Configuration Note*.

# Required Base Configuration

A typical HA configuration requires that you define interfaces in three directions: PDSN/FA, home network, and AAA server. If HA redundancy is required, then you must configure another interface for HSRP binding updates between HAs. If you are running the HA on the MWAM, the HA will see the access to one GE port that will connect to Catalyst 6500 backplane. That port can be configured as a trunk port with subinterfaces provided for each necessary network access.

VLANs can be defined corresponding to each interface: PDSN/FA, home network, AAA. In the case of multiple HA instances in the same Catalyst 6500 chassis, or 7600 chassis, the same VLAN can be used for all of them.

The following sections illustrate the required base configuration for the Cisco Mobile Wireless Home Agent:



## Basic IOS Configuration on MWAM

To configure the Supervisor engine to recognize the MWAM modules, and to establish physical connections to the backplane, use the following commands:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `router# vlan database` | Enter VLAN configuration mode. |
| **Step 2** | `router(vlan)# vlan vlan-id` | Add an Ethernet VLAN. |
| **Step 3** | `router(vlan)# exit` | Updates the VLAN database, propagates it throughout the administrative domain, and return to privileged EXEC mode. |
| **Step 4** | `router(config)# mwam module 7 port 3 allowed-vlan vlan_range` | Configures the ethernet connectivity from the backplane to the individual processors on the MWAM. |
| **Step 5** | `router# session slot MWAM module processor processor number` | Configures the ethernet connectivity from the backplane to the individual processors on the MWAM. ***Processor number* is from 2 to 6**. |
| **Step 6** | `Router(config)# int gigabitEthernet 0/0` | Specifies the type of interface being configured, and the slot number. |
| **Step 7** | `Router(config-if)# no shut` | Puts the specified GE interfaces in service. |

| | Command | Purpose |
|---|---|---|
| **Step 8** | `Router(config-if)# int gigabitEthernet 0/0.401` | Specifies the type of interface being configured, and the slot number. |
| **Step 9** | `Router(config-subif)# encapsulation dot1Q 401` | Enables IEEE 802.1Q encapsulation of traffic on a specified sub interface in virtual LANs. |
| **Step 10** | `Router(config-subif)# ip address 10.1.1.1 255.255.255.0` | Specifies the IP address. |
| **Step 11** | `Router(config-subif)# exit` | Updates the VLAN database, propagates it throughout the administrative domain, and return to privileged EXEC mode. |

**Note** MWAM modules synchronize their timing functions from the Supervisor engine's clock timers. Do not configure the timers on each individual MWAM.

## Configuring AAA in the Home Agent Environment

Access control is the way you manage who is allowed access to the network server and what services they are allowed to use. AAA network security services provide the primary framework through which you set up access control on your router or access server. For detailed information about AAA configuration options, refer to the "Configuring Authentication," and "Configuring Accounting" chapters in the *Cisco IOS Security Configuration Guide*.

To configure AAA in the HA environment, use the following commands in global configuration mode:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Router(config)# aaa authentication ppp default group radius` | Enables authentication of PPP users using RADIUS. |
| **Step 1** | `Router(config)# aaa authorization network default group radius` | Restricts network access to a user. Runs authorization for all network-related service requests. Uses the group radius authorization method as the default method for authorization. |

## Configuring RADIUS in the Home Agent Environment

RADIUS is a method for defining the exchange of AAA information in the network. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a RADIUS server that contains all user authentication and network server access information. For detailed information about RADIUS configuration options, refer to the "Configuring RADIUS" chapter in the *Cisco IOS Security Configuration Guide*.

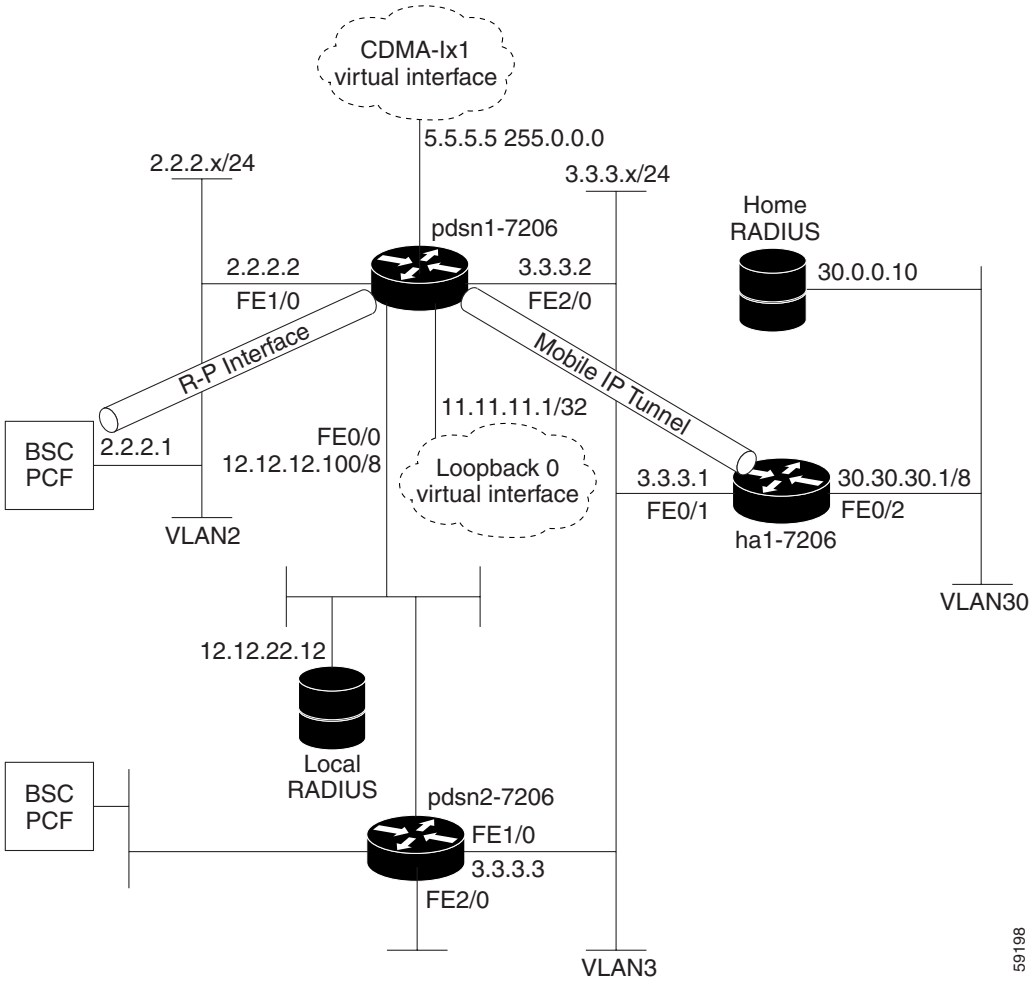
To configure RADIUS in the HA environment, use the following commands in global configuration mode:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Router(config)# radius-server host ip-addr key sharedsecret` | Specifies the IP address of the RADIUS server host and specifies the shared secret text string used between the router and the RADIUS server. |

# Configuration Examples

Figure 1-1 and the information that follows is an example of the placement of a Cisco HA and it's configuration.

*Figure 1-1 Home Agent —A Network Map*




**Example 1**

```
hostname ha1-7206
!
aaa new-model
!
aaa authentication login default group radius
aaa authentication login CONSOLE none
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa session-id common
!
interface FastEthernet0/1
 description To FA/PDSN
 ip address 3.3.3.1 255.255.255.0
!
interface FastEthernet0/2
 description To AAA
 ip address 10.30.30.1 255.0.0.0
!
router mobile
!
```

```
ip local pool ha-pool1 10.35.35.1 35.35.35.254
ip mobile home-agent broadcast
ip mobile virtual-network 10.35.35.0 255.255.255.0
ip mobile host nai @xyz.com address pool local ha-pool1 virtual-network 10.35.35.0
255.255.255.0 aaa load-sa lifetime 65535
!
radius-server host 10.0.0.10 auth-port 1645 acct-port 1646 key cisco
!
line con 0
 exec-timeout 0 0
 login authentication CONSOLE
```

---

### *Example 1-1 Home Agent Configuration*

```
Cisco_HA#sh run
Building configuration...

Current configuration : 4532 bytes
!
version 12.2
no parser cache
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service udp-small-servers
service tcp-small-servers
!
hostname USER_HA
!
aaa new-model
!
!
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa authorization configuration default group radius
aaa session-id common
!
username simulator password 0 cisco
username userc-moip password 0 cisco
username pdsn password 0 cisco
username userc password 0 cisco
username USER_PDSN
ip subnet-zero
ip cef
!
!
no ip domain-lookup
!
! !
!
 interface Loopback0
 ip address 10.2.2.2 255.255.255.0
!
interface Tunnel1
 no ip address
!
```

```
interface FastEthernet0/0
 ip address 10.15.68.14 255.255.0.0
 duplex half
 speed 100
 no cdp enable
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex half
 speed 10
 no cdp enable
!
interface FastEthernet1/0
 ip address 10.92.92.2 255.255.0.0
 duplex auto
 speed auto
 no cdp enable
!
interface FastEthernet1/1
 ip address 10.5.5.3 255.255.255.0 secondary
 ip address 10.5.5.1 255.255.255.0
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
!
router mobile
!
ip local pool ha-pool 10.0.0.1 10.0.15.254
ip local pool ha-pool1 10.4.4.100 10.4.4.255
ip default-gateway 10.15.0.1
ip classless
ip route 10.3.3.1 255.255.255.255 FastEthernet1/1
ip route 10.100.0.1 255.255.255.255 9.15.0.1
ip route 10.17.17.17 255.255.255.255 FastEthernet1/0
no ip http server
ip pim bidir-enable
ip mobile home-agent
ip mobile host nai userc-moip address pool local ha-pool interface FastEthernet1/0
ip mobile host nai userc address pool local pdsn-pool interface Loopback0 aaa
ip mobile secure host nai userc-moip spi 100 key hex ffffffffffffffffffffffffffffffff
replay timestamp within 150
!
!
radius-server host 10.15.200.1 auth-port 1645 acct-port 1646 key cisco
radius-server retransmit 3
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!

gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
line aux 0
```

```
line vty 5 15
!
!
end
```

# Restrictions

### Simultaneous Bindings

The Cisco Home Agent does not support simultaneous bindings. When multiple flows are established for the same NAI, a different IP address is assigned to each flow. This means that simultaneous binding is not required, because it is used to maintain more than one flow to the same IP address.

### Security

The HA supports IPSec, IKE, IPSec Authentication Header (AH) and IP Encapsulating Security Payload (ESP) as required in IS-835-B. The Home Agent does not support security for control or user traffic independently. Either both are secured, or neither.

The Home Agent does not support dynamically assigned keys or shared secrets as defined in IS-835-B.

# Supported Standards, MIBs, and RFCs

### RFCs

Cisco IOS Mobile Wireless Home Agent Release 3.0 supports the following RFCs:

- IPv4 Mobility, RFC 2002
- IP Encapsulation within IP, RFC 2003
- Applicability Statement for IP Mobility Support, RFC 2005
- The Definitions of Managed Objects for IP Mobility Support Using SMIv2, RFC 2006
- Reverse Tunneling for Mobile IP, RFC 3024
- Mobile IPv4 Challenge/Response Extensions, RFC 3012
- Mobile NAI Extension, RFC 2794
- Generic Routing Encapsulation, RFC 1701
- GRE Key and Sequence Number Extensions, RFC 2890
- IP Mobility Support for IPv4, RFC 3220, Section 3.2 Authentication
- The Network Access Identifier, RFC 2486, January 1999.
- An Ethernet Address Resolution Protocol, RFC 826, November 1982
- The Internet Key Exchange (IKE), RFC 2409, November 1998.
- Cisco Hot Standby Routing Protocol (HSRP), RFC 2281, March 1998

### Standards

Cisco IOS Mobile Wireless Home Agent Release 3.0 supports the following standards:

- TIA/EIA/IS-835-B, TIA/EIA/IS-835-C and TIA/EIA/IS-835-D

### MIBs

Cisco IOS Mobile Wireless Home Agent Release 3.0 supports the following MIBs:

- CISCO- MOBILE-IP-MIB—provides enhanced management capabilities.
- Radius MIB—as defined in RADIUS Authentication Client MIB, RFC 2618, June 1999.

The HA implements SNMPv2 as specified in the suite of protocols: RFC 1901 to RFC 1908. The HA supports the MIB defined in The Definitions of Managed Objects for IP Mobility Support Using SMIv2, RFC 2006, October 1995.

A full list of MIBs that are supported on the 7200, 7600 and 6500 series platforms can be found on Cisco web at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Session counters maintained in the MIB cannot be reset using SNMP or CLI. The Home Agent CPU and Memory Utilization counters are accessible using the CISCO-PROCESS-MIB.

The following additional counters will be supported in the Cisco Mobile Wireless Home Agent Release 3.0 MIB:

- Number of Bindings for FA/CoA
- Number of registration requests received per FA/CoA
- Failure counters per FA/CoA—HA Release 2.0 and above supports global failure counters. A per-FA/CoA counter will be added for each of those counters

# Related Documents

### Cisco IOS Software Documentation

- *Cisco IOS Dial Technologies Configuration Guide*, Release 12.3
- *Cisco IOS Dial Technologies Command Reference*, Release 12.3
- *Cisco IOS Interface Configuration Guide*, Release 12.3
- *Cisco IOS Interface Command Reference*, Release 12.3
- *Cisco IOS IP Configuration Guide*, Release 12.3
- *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*, Release 12.3
- Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.3
- Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.3
- *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.3
- *Cisco IOS Quality of Service Solutions Command Reference*, Release 12.3
- *Cisco IOS Security Configuration Guide*, Release 12.3

- *Cisco IOS Security Command Reference*, Release 12.3
- *Cisco IOS Switching Services Configuration Guide*, Release 12.3
- *Cisco IOS Switching Services Command Reference*, Release 12.3
- *Cisco Multi-Processor WAN Application Module Installation and Configuration Note*

CHAPTER 1

# Assigning a Home Address on the Home Agent

This chapter discusses how the Cisco Mobile Wireless Home Agent assigns home addresses to a mobile note, the different address types, and provides configuration details and examples.

This chapter includes the following sections:



## Home Address Assignment

The Home Agent assigns a home address to the mobile node based on user NAI received during Mobile IP registration. The IP addresses assigned to a mobile station may be statically or dynamically assigned. The Home Agent does not permit simultaneous registrations for different NAIs with the same IP address, whether it is statically or dynamically assigned.

### Static IP Address

A static IP address is an address that is pre-assigned to the mobile station, and possibly preconfigured at the mobile device. The Home Agent supports static addresses that might be public IP addresses, or addresses in a private domain.

**Note** Use of private addresses for Mobile IP services requires reverse tunneling between the PDSN/FA and the Home Agent.

The mobile user proposes the configured or available address as a non-zero home address in the registration request message. The Home Agent may accept this address, or return another address in the registration reply message. The Home Agent may obtain the IP address by accessing the home AAA server or DHCP server. The home AAA server may return the name of a local pool, or a single IP address. On successful Mobile IP registration, Mobile IP based services are made available to the user.

## Static Home Addressing Without NAI

The original Mobile IP specification supported only static addressing of mobile nodes. The home IP address served as the "user name" portion of the authentication. Static addressing can be beneficial because it allows each device to keep the same address all the time no matter where it is attached to the network. This allows the user to run mobile terminated services without updating the DNS, or some other form of address resolution. It is also easy to manage MNs with static addressing because the home address and the Home Agent are always the same. However, provisioning and maintenance are much more difficult with static addressing because address allocation must be handled manually, and both the Home Agent and MN must be updated. Here is an example configuration:

```
router (config)# ip mobile host 10.0.0.5 interface FastEthernet0/0
router (config)# ip mobile host 10.0.0.10 10.0.0.15 interface FastEthernet0/0
router (config)# ip mobile secure host 10.0.0.12 spi 100 key ascii secret
```

## Static Home Addressing with NAI

Static home addressing can also be used in conjunction with NAI to support an NAI-based authorization and other services. It is also possible to allow a single user to use multiple static IP addresses either on the same device, or multiple devices, while maintaining only one AAA record and security association. A user must be authorized to use an address before the registration will be accepted. Addresses can be authorized either locally, or through a AAA server. If a MN requests an address which is already associated with a binding that has a different NAI, the HA will attempt to return another address from the pool unless the command is set.

Here is a sample configuration:

```
router (config)# ip mobile home-agent reject-static-addr
```

## Local Authorization

A static address can be authorized on a per MN or per realm basis using configuration commands. Per MN configurations require that you define a specific NAI in the *user* or *user@realm* form. Per realm configurations require that you define a generic NAI in the *@realm* form, and allow only the specification of a local pool.

Here is a sample configuration:

```
router (config)# ip local pool static-pool 10.0.0.5 10.0.0.10
router (config)# ip mobile host nai user@staticuser.com static-address 10.0.0.1 10.0.0.2
   interface FastEthernet0/0
router (config)# ip mobile host nai user@staticuser.com static-address local-pool
   static-pool interface FastEthernet0/0
router (config)# ip mobile host nai @static.com static-address local-pool static-pool
   interface FastEthernet0/0
```

## AAA Authorization

It is also possible to store either the authorized addresses, or local pool name in a AAA server. Each user must have either the **static-ip-addresses** attribute or the **static-ip-pool** attribute configured in the AAA server. Unlike the static address configuration on the command line, the **static-ip-addresses** attribute is not limited in the number of addresses that can be returned.

Here is a sample configuration.

HA configuration:

```
router (config)# ip local pool static-pool 10.0.0.5 10.0.0.10
router (config)# ip mobile host nai user@staticuser.com interface FastEthernet0/0 aaa
router (config)# ip mobile host nai @static.com interface FastEthernet0/0 aaa
```

Radius Attributes:

Cisco-AVPair = “mobileip:static-ip-addresses=10.0.0.1 10.0.0.2 10.0.0.3”

Cisco-AVPair = “mobileip:static-ip-pool=static-pool”

# Dynamic Home Agent Assignment

The Home Agent can be dynamically assigned in a CDMA2000 network when the following qualifications exist:

- The first qualification is that the Home Agent receives a Mobile IP registration request with a value of 0.0.0.0 in the Home Agent field. Upon authentication/authorization, the PDSN retrieves the HA’s IP address. The PDSN then uses this address to forward the Registration Request to the HA, but does not update the actual HA address field in the Registration Request.

  The Home Agent sends a Registration Reply, and places it’s own IP address in the Home Agent field. At this point, any re-registration requests that are received would contain the Home Agent’s IP address in the Home Agent field.

- The second qualification is a function of the PDSN/Foreign Agent, and is included here for completeness. In this case, a AAA server is used to perform the dynamic Home Agent assignment function. Depending on network topology, either the local-AAA, or the home-AAA server would perform this function. When an access service provider is also serving as an ISP, Home Agents would be located in the access provider network. In this service scenario, a local-AAA server would perform Home Agent assignment function. Based on the user NAI received in the access request message, the AAA server would return an elected Home Agent’s address in an access reply message to the PDSN.

  A pool of Home Agent addresses is typically configured at the AAA server. For the access provider serving as an ISP, multiple pools of Home Agents could be configured at the local AAA server; however, this depends on SLAs with the domains for which Mobile IP, or proxy-Mobile IP services are supported. You can configure the Home Agent selection procedure at the AAA server, using either a round-robin or a hashing algorithm over user NAI selection criteria.

The PDSN/Foreign Agent sends the Registration Request to the Home Agent; however, there is no IP address in the HA field of the MIP RRQ (it is 0.0.0.0). When the PDSN retrieves the IP address from AAA, it does not update the MIP RRQ; instead, it forwards the RRQ to the HA address retrieved. The PDSN cannot alter the MIP RRQ because it does not know the MN-HA SPI, and key value (which contains the IP address of the Home Agent in the "Home Agent" field). Depending on network topology, either the local AAA, or the home AAA server would perform this function. In situations where the Home Agents are located in the access provider network, the local AAA server would perform Home Agent assignment function. Additionally, multiple pools of Home Agents could be configured at the local AAA server, depending on SLAs with the domains for which Mobile IP, or proxy Mobile IP services are supported.

# Dynamic IP Address

It is not necessary for a home IP address to be configured in the mobile station to access packet data services. A mobile user may request a dynamically assigned address by proposing an all-zero home address in the registration request message. The Home Agent assigns a home address and returns it to the MN in the registration reply message. The Home Agent obtains the IP address by accessing the home AAA server. The AAA server returns the name of a local pool or a single IP address. On successful registration, Mobile IP based services are made available to the user.

## Fixed Addressing

It is possible to configure the Home Agent with a fixed address for each NAI. The fixed address is assigned to the MN each time it registers. This provides users all the benefits of static addressing while simplifying the configuration of the MN.

**Note** We do not recommend fixed addressing for large-scale deployment because the Home Agent configuration must be updated to perform all user maintenance.

Here is a sample configuration:

```
router# ip mobile host nai user@realm.com address 10.0.0.1 interface FastEthernet0/0
```

## Local Pool Assignment

Local pool assignment requires that one or more address pools be configured on the HA. The HA allocates addresses from the pool on a first come, first served basis. The MN will keep the address as long as it has an active binding in the HA. The MN may update it's binding by sending a RRQ with either the allocated address, or 0.0.0.0 as it's home address. When the binding expires the address is immediately returned to the pool.

**Note** Currently local pool allocation cannot be used with the peer-to-peer HA Redundancy model. The number of local pools that you can configure is limited only by the available memory on the router.

Here is a sample configuration:

```
router (config)# ip local pool mippool 10.0.0.5 10.0.0.250
router (config)# ip mobile host nai @localpool.com address pool local mippool
virtual-network 10.0.0.0 255.255.255.0
```

### SNMP Traps to Track Utilization of Local IP Pool

The CISCO-IP-LOCAL-POOL-MIB has traps to track local pool utilization, but these traps require that you specify the threshold in absolute numbers. However, it is desirable to track pool utilization in percentage when there are several, non-contiguous, IP pools. Cisco IOS Release 12.4(11)T adds the following required capabilities:

- A new *threshold* option is added to the **ip local pool** command to configure high and low threshold in percentage terms. Objects "cIpLocalPoolPercentAddrThldLo" and "cIpLocalPoolPercentAddrThldHi" are defined for the high and low threshold watermark, respectively.
- A notification object "cIpLocalPoolPercentAddrThldHi" is defined. When the percentage of used addresses in an IP local pool is equal to (or exceeds) the "cIpLocalPoolPercentAddrThldHi" threshold value, the "ciscoIpLocalPoolPercentAddrNoti" notification is generated. Once this notification is generated, it is disarmed and is not generated again until the number of used address falls below the value indicated by "cIpLocalPoolPercentAddrThldLo". When the percentage of used addresses in the IP local pool falls below the "cIpLocalPoolPercentAddrThldLo" threshold value, the "ciscoIpLocalPoolPercentAddrNoti" notification is rearmed.

## DHCP Allocation

The Dynamic Host Configuration Protocol (DHCP) is widely used to allocate IP addresses for desktop computers. IOS Mobile IP leverages the existing DHCP proxy client in IOS to allow the home address to be allocated by a DHCP server. The NAI is sent in the Client-ID option, and can be used to provide dynamic DNS services.

Here is a sample configuration:

```
router(config)# ip mobile host nai @dhcppool.com address pool dhcp-proxy-client
dhcp-server 10.1.2.3 interface FastEthernet 0/0
```

**Note** Currently DHCP cannot be used with the peer-to-peer HA redundancy model.

## Dynamic Addressing from AAA

Dynamic addressing from AAA allows you to support fixed and/or per session addressing for MNs without the trouble of maintaining addressing at the MN or HA. The AAA server can return either a specific address, a local pool name, or a DHCP server address. If the AAA server is used to return a specific address, the home address can be configured either as an attribute on the NAI entry in the RADIUS database, or can be allocated from a pool depending on the capabilities of the AAA server being used. The AAA server can also return the name of a local pool configured on the HA or a DHCP server IP address.

Here is a sample configuration.

On the HA:

```
router (config)# ip local pool dynamic-pool 10.0.0.5 10.0.0.10
router (config)# ip mobile host nai user@staticuser.com interface FastEthernet0/0 aaa
router (config)# ip mobile host nai @static.com interface FastEthernet0/0 aaa
```

AAA Address assignment:
Cisco-AVPair = “mobileip:ip-address=65.0.0.71”

AAA Local Pool attribute:
Cisco-AVPair = “mobileip:ip-pool=dynamic-pool”

AAA DHCP server attribute:
Cisco-AVPair = “mobileip:dhcp-server=10.1.5.10”

# On-Demand Address Pool (ODAP)

If you use MWAM cards to provide a higher density of HAs, you may choose to have IP addresses allocated from a central source. Cisco’s IOS On-Demand Address Pools (ODAPs) provides this functionality. ODAP simplifies HA configuration, in that you will not have to configure a local pool of IP addresses in each HA configuration.

You can use ODAP to centralize the management of large pools of addresses and simplify the configuration of large networks. The ODAP feature consists of two components:

- DHCP ODAP subnet allocation server
- ODAP manager (residing on each HA)

A DHCP ODAP subnet allocation server is configured to create and allocate pools of IP address space on a per-subnet basis. The size of these pools is configurable, and these subnets will be leased to the ODAP managers on the HA, and they provide subnet allocation pools for the ODAP manager allocation. The DHCP ODAP subnet allocation server functionality can reside on one of the HA instances on the MWAM. The DHCP ODAP subnet allocation server functionality can also reside on another external Cisco IOS router, or an external Cisco Access Register.

The ODAP manager functionality resides on each HA image. Rather than using local IP pools, the HA uses the ODAP manager functionality. The ODAP manager leases subnets from the ODAP subnet allocation server based on the demand for IP addresses and subnet availability to each HA. The ODAP manager on the HA assigns addresses to clients from these subnets, and dynamically increases or decreases the subnet pool size depending on address utilization. When an HA ODAP manager leases a subnet, a summarized route is automatically added for each subnet that the HA receives. This route is added to the Null interface and is a static route.

When the ODAP manager on the HA allocates a subnet, the ODAP subnet allocation server creates a subnet binding. This binding is stored in the DHCP database for as long as the ODAP manager needs the address space. The binding is destroyed and the subnet returned to the subnet pool only when the HA ODAP manager releases the subnet as the address space utilization decreases.

The DHCP ODAP subnet allocation server has enhanced DHCP functionality. Instead of returning a single IP address, it returns a subnet of addresses. The ODAP manager manages this pool of IP addresses on the HA. This functionality provides a more efficient route summarization for the routing protocols.

# Configuring ODAP-based Address Allocation

To enable the HA to support ODAP pools, perform the following task:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Router(config)# ip mobile host` *nai* `address pool dhcp-pool` *odap poolname* | Enables the HA to support ODAP address pools. |

Here is an example:

Router (config)#**ip mobile host nai** @ispbar2.com address pool dhcp-pool ha-dhcp-pool

## ODAP Restrictions

The following restrictions apply to the ODAP feature:

- ODAP with peer-to-peer redundancy is not supported.
- The minimum subnet lease time on the ODAP server must be 10 minutes.
- Preemption with rf-interdev support is not working.

## Address Assignment for Same NAI - Multiple Static Addresses

The Cisco Home Agent supports multiple Mobile IP registrations for the same NAI with different static addresses. This is accomplished by configuring static-ip-address pool(s) at the home-AAA or DHCP server. When the HA receives a Registration Request message from the mobile user, the HA accesses the home-AAA for authentication, and possibly for assignment of an IP address. The NAI provided by the mobile user is sent to the home-AAA. The home-AAA server returns a list of static-IP-addresses or the static-ip-pool name corresponding to this NAI.

## Address Assignment For Same NAI - Different Mobile Terminal

When the same NAI is used for registration from two different mobiles, the behavior is as follows:

- If static address assignment is used in both cases, they are viewed as independent cases.
- If dynamic address assignment is used in both cases, the second registration replaces the first.
- If static is used for the first, and dynamic for the second, the dynamic address assignment replaces the static address assignment.
- If dynamic is used for the first, and static for the second, they are viewed as independent cases.

Additionally, two flows originating from the same mobile using the same NAI—but two different Home Agents—are viewed as independent cases.

# Configuration Examples

## ODAP Redundancy Configuration

**Active-HA configuration**

```
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mwt10-7206b
!
redundancy inter-device
 scheme standby cisco
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 500
    local-ip 10.0.0.2
   remote-port 500
    remote-ip 10.0.0.3
aaa new-model
!
aaa authentication ppp default local group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa session-id common
!
ip dhcp ping packet 0
ip dhcp pool ha-dhcp-pool
   origin dhcp subnet size initial /30 autogrow /30
ip subnet-zero
ip cef
!
interface Ethernet2/0
 description to PDSN/FA
 ip address 10.0.0.2 255.0.0.0
 no ip route-cache
 no ip mroute-cache
 duplex half
 standby ip 10.0.0.4
 standby priority 110
 standby preempt delay min 100
 standby name cisco
!
interface Ethernet2/2
 description to AAA
 ip address 172.16.1.8 255.255.0.0
 no ip route-cache
 no ip mroute-cache
 duplex half
!
router mobile
!
ip classless
```

```
no ip http server
ip pim bidir-enable
ip mobile home-agent
ip mobile home-agent redundancy cisco
ip mobile virtual-network 33.0.0.0 255.0.0.0
ip mobile host nai user14@cisco.com address pool dhcp-pool ha-dhcp-pool
virtual-network 10.0.0.0 255.0.0.0 aaa
ip mobile secure home-agent 10.0.0.3 spi 100 key ascii redundancy
algorithm md5 mode
prefix-suffix
!
radius-server host 172.16.0.2 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
gatekeeper
 shutdown
!
line con 0
line aux 0
line vty 0 4
!
end
```

### Standby-HA configuration

```
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mwt10-7206b
!
redundancy inter-device
 scheme standby cisco
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 500
    local-ip 10.0.0.3
   remote-port 500
    remote-ip 10.0.0.2
aaa new-model
!
aaa authentication ppp default local group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa session-id common
!
ip dhcp pool ha-dhcp-pool
   origin dhcp subnet size initial /30 autogrow /30
ip subnet-zero
ip cef
```

```
!
interface Ethernet2/0
 description to PDSN/FA
 ip address 10.0.0.3 255.0.0.0
 no ip route-cache
 no ip mroute-cache
 duplex half
 standby ip 10.0.0.4
 standby name cisco
!

interface Ethernet2/2
 description to AAA
 ip address 150.2.1.7 255.255.0.0
 no ip route-cache
 no ip mroute-cache
 duplex half
!

router mobile
!
ip classless
no ip http server
ip pim bidir-enable
ip mobile home-agent
ip mobile home-agent redundancy cisco
ip mobile virtual-network 10.0.0.0 255.0.0.0
ip mobile host nai user14@cisco.com address pool dhcp-pool ha-dhcp-pool
virtual-network 10.0.0.0 255.0.0.0 aaa
ip mobile secure home-agent 10.0.0.2 spi 100 key ascii redundancy
algorithm md5 mode
prefix-suffix
!
radius-server host 172.16.0.2 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
gatekeeper
 shutdown
!
line con 0
line aux 0
line vty 0 4
!
end
```

# DHCP-Proxy-Client Configuration

### Active-HA configuration

```
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mwt10-7206b
```

```
!
aaa new-model
!
aaa authentication ppp default local group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa session-id common
!
ip subnet-zero
ip cef
!
interface Loopback0
ip address 10.0.0.1 255.255.255.255
interface Ethernet2/0
 description to PDSN/FA
 ip address 10.0.0.2 255.0.0.0
 no ip route-cache
 no ip mroute-cache
 duplex half
 standby ip 10.0.0.4
 standby priority 110
 standby preempt delay sync 100
 standby name cisco
!
interface Ethernet2/2
 description to AAA
 ip address 172.16.1.8 255.255.0.0
 no ip route-cache
 no ip mroute-cache
 duplex half
!
router mobile
!
ip classless
no ip http server
ip pim bidir-enable
ip mobile home-agent
ip mobile home-agent redundancy cisco
ip mobile virtual-network 10.0.0.0 255.0.0.0
ip mobile host nai user01@cisco.com address pool dhcp-proxy-client
dhcp-server 10.0.0.101 virtual-network 10.0.0.0 255.0.0.0
ip mobile secure home-agent 10.0.0.3 spi 100 key ascii redundancy
algorithm md5 mode
prefix-suffix
!
ip mobile virtual-network 10.0.0.0 255.0.0.0
ip mobile host nai user01@cisco.com address pool dhcp-proxy-client
dhcp-server 10.0.0.101 virtual-network 10.0.0.0 255.0.0.0
radius-server host 172.16.0.2 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
gatekeeper
 shutdown
!
line con 0
line aux 0
line vty 0 4
```

```
!
end
```

### Standby-HA configuration

```
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mwt10-7206b
!
aaa new-model
!
aaa authentication ppp default local group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa session-id common
!
ip subnet-zero
ip cef
!
interface Loopback0
ip address 10.0.0.2 255.255.255.255
interface Ethernet2/0
 description to PDSN/FA
 ip address 10.0.0.3 255.0.0.0
 no ip route-cache
 no ip mroute-cache
 duplex half
 standby ip 10.0.0.4
 standby name cisco
!
interface Ethernet2/2
 description to AAA
 ip address 172.16.1.7 255.255.0.0
 no ip route-cache
 no ip mroute-cache
 duplex half
!
router mobile
!
ip local pool ha-pool 10.0.0.1 10.0.0.255
ip classless
no ip http server
ip pim bidir-enable
ip mobile home-agent
ip mobile home-agent redundancy cisco
ip mobile secure home-agent 10.0.0.2 spi 100 key ascii redundancy
algorithm md5 mode
prefix-suffix
ip mobile virtual-network 10.0.0.0 255.0.0.0
ip mobile host nai user01@cisco.com address pool dhcp-proxy-client
dhcp-server 10.0.0.101 virtual-network 10.0.0.0 255.0.0.0
!
radius-server host 150.2.0.2 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
call rsvp-sync
!
mgcp profile default
```

```
!
dial-peer cor custom
!
gatekeeper
 shutdown
!
line con 0
line aux 0
line vty 0 4
!
end
```

CHAPTER 1

# User Authentication and Authorization

This chapter discusses User Authentication and Authorization, and how to configure this feature on the Cisco Mobile Wireless Home Agent.

This chapter includes the following sections:



## User Authentication and Authorization

You can configure the Home Agent to authenticate a user with either Password Authentication Protocol (PAP), or Challenge Handshake Authentication Protocol (CHAP). The Foreign Agent Challenge procedures are supported (RFC 3012) and include the following extensions:

- Mobile IP Agent Advertisement Challenge Extension
- MN-FA Challenge Extension
- MN-AAA Authentication Extension

**Note** PAP is used if no MN-AAA extension is present, and CHAP is always used if MN-AAA is present. The password for PAP users can be set using the **ip mobile home-agent aaa user-password** command.

If the Home Agent receives the MN-AAA Authentication Extension in the Registration Request (when configured to authenticate the user with the Home AAA-server), the contents are used. If the extension is absent, a default configurable password is used. This default password is a locally defined string such as “vendor”.

The HA accepts and maintains the MN-FA challenge extension and MN-AAA authentication extension (if present) from the original registration for use in later registration updates.

If the Home Agent does not receive a response from the AAA server within a configurable timeout, the message can be retransmitted a configurable number of times. You can configure the Home Agent to communicate with a group of AAA servers; the server is chosen in round-robin fashion from the available configured servers.

To configure authorization and authentication on the HA, perform the following tasks:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Router(config)#` **ip mobile host** {*lower* [*upper*] \| nai string {static-address {addr1 [addr2] [addr3] [addr4] [addr5] \| local-pool name} \| address {addr \| pool {local name \| dhcp-proxy-client [**dhcp-server** *addr*]} {**interface** *name* \| **virtual-network** *network_address mask*} [**skip-chap \| aaa** [**load-sa** [permanent]] [authorized-pool pool name] [skip-aaa-reauthentication] [**care-of-access** *acl*] [**lifetime** *seconds*] | Configures the mobile host or mobile node group on the HA.<br>If the **aaa load-sa** option is configured, the Home Agent caches the SA locally on first registration. In this case the Home Agent will not invoke the RADIUS authorization procedure for re-registration.<br>If **aaa load-sa skip-aaa-reauthentication** is configured, the Home Agent caches the SA locally on first registration; however, the Home Agent will not invoke HA-CHAP procedure for re-registration.<br>The **aaa load-sa permanent** option is not supported on the Mobile Wireless Home Agent, and should not be configured. |

The HA supports 3GPP2 and Cisco proprietary security extension attributes in RADIUS access accept packet. Sending 3GPP2 MN-HA SPI in Access Request to RADIUS server and processing the MN-HA Secure Key Received from RADIUS server is configurable on HA.

Cisco IOS provides a mechanism to authorize subscribers based on their realm. This can be done using a feature called “Subscriber Authorization”, the details of which can be found here: http://www.cisco.com/en/US/partner/products/ps6350/products_configuration_guide_chapter09186a0080455cf0.html#wp1056463.

**Note** The Home Agent will accept user profiles, it will not authorize a mobile subscriber based on information returned in a group profile.

# Skip HA-CHAP with MN-FA Challenge Extension (MFCE)

This feature allows the HA to download a Security Association (SA) and cache it locally on the disk, rather than performing a HA-CHAP procedure with Home AAA server to download the SA for the user for each registration request. When a user first registers with the HA, the HA does HA-CHAP (MN-AAA authentication), downloads the SA, and caches it locally. On subsequent re-registration requests, the HA uses the locally cached SA to authenticate the user. The SA cache entry is removed when the binding for the user is deleted.

You can configure this feature on the HA using the **ip mobile host** command, noted above.

# Configuration Examples

The following example configures a mobile node group to reside on virtual network 10.99.1.0 and retrieve and cache mobile node security associations from a AAA server. The cached security association is then used for subsequent registrations.

```
ip mobile host 10.99.1.1 10.99.1.100 virtual-network 10.99.1.0 aaa load-sa
```

The following example configures a local pool of dynamic addresses to be used in assigning IP addresses to mobile nodes in the cisco.com domain. The security associations that are retrieved from the AAA server are cached permanently until cleared manually.

```
ip mobile host nai @cisco.com address pool local mobilenodes virtual network 10.2.0.0
255.255.0.0 aaa load-sa permanent lifetime 180
```

# Authentication and Authorization RADIUS Attributes

The Home Agent, and the RADIUS server support RADIUS attributes listed in Table 1-1 for authentication and authorization services.

*Table 1-1 Authentication and Authorization AVPs Supported by Cisco IOS*

| Authentication and Authorization AVPs Supported By Cisco IOS Name | Type | Vendor | Length | Format | Description | Allowed In Access Request | Allowed In Access Accept |
|---|---|---|---|---|---|---|---|
| User-Name | 1 | NA | 64 | string | User name for authentication and authorization. | Yes | No |
| User-Password | 2 | NA | >=18 && <=130 | string | Password for authentication when using PAP.<br>Password configured using CLI at Home Agent. | Yes | No |
| CHAP-Password | 3 | NA | 19 | string | CHAP password | Yes | No |
| NAS-IP-Address | 4 | NA | 4 | IP address | IP address of the HA interface used for communicating with RADIUS server. | Yes | No |
| Service Type | 6 | NA | 4 | integer | Type of service the user receives.<br>Supported values:<br>• Outbound sent for PAP<br>• Framed sent for CHAP<br>• Framed received in both cases | Yes | Yes |
| Framed-Protocol | 7 | NA | 4 | integer | Framing protocol user is using. Sent for CHAP, received for PAP and CHAP.<br>Supported values:<br>• PPP | Yes | Yes |

*Table 1-1 Authentication and Authorization AVPs Supported by Cisco IOS (continued)*

| Authentication and Authorization AVPs Supported By Cisco IOS Name | Type | Vendor | Length | Format | Description | Allowed In Access Request | Allowed In Access Accept |
|---|---|---|---|---|---|---|---|
| Framed Compression | 13 | NA | 4 | integer | Compression method<br>Supported values:<br>• 0 - None | No | Yes |
| Framed-Routing | 10 | NA | 4 | integer | Routing method<br>Supported values:<br>• 0 - None | No | Yes |
| Vendor Specific | 26 | NA | | | Vendor specific attributes | Yes | Yes |
| CHAP-Challenge (optional) | 60 | NA | >=7 | string | CHAP Challenge | Yes | No |
| NAS-Port-Type | 61 | NA | 4 | integer | Port Type<br>Supported:<br>• 0 - Async | Yes | No |
| spi#*n* | 26/1 | Cisco | >=3 | string | *n* is a numeric identifier beginning with **0** that allows multiple SAs per user.<br>Provides the Security Parameter Index (SPI), for authenticating a mobile user during MIP registration.<br>The information is in the same syntax as the **ip mobile secure host** *addr* configuration command. Essentially, it contains the rest of the configuration command that follows that string, verbatim. | No | Yes |
| static-ip-addresses | 26/1 | Cisco | >=3 | string | IP address list for static addresses for same NAI but multiple flows. | No | Yes |
| static-ip-pool | 26/1 | Cisco | >=3 | string | IP address pool name for static address for same NAI with multiple flows. | No | Yes |
| ip-addresses | 26/1 | Cisco | >=3 | string | IP address list used for dynamic address assignment. | No | Yes |
| ip-pool | 26/1 | Cisco | >=3 | string | IP address pool name used for dynamic address assignment. | No | Yes |
| dhcp-server | 26/1 | Cisco | >=3 | string | Get an address from the specified DHCP server. | No | Yes |
| MN-HA SPI Key | 26/57 | 3GPP2 | 6 | integer | SPI for MN HA Shared Key. | Yes | No |
| MN-HA Shared Key | 26/58 | 3GPP2 | 20 | string | Secure Key to authenticate MHAE. | No | Yes |

CHAPTER 1

# Home Agent Redundancy

This chapter discusses several concepts related to Home Agent Redundancy, how Home Agent redundancy works, and how to configure redundancy on the Cisco Mobile Wireless Home Agent.

This chapter includes the following sections:



## Overview of Home Agent Redundancy

Cisco Home Agents can be configured to provide 1:1 redundancy. Two Home Agents are configured in hot-standby mode, based on Cisco Hot Standby Routing Protocol (HSRP in RFC 2281). This enables the active Home Agent to continually copy mobile session-related information to the standby Home Agent, and maintains synchronized state information at both Home Agents. In case an active Home Agent fails, the standby Home Agent takes over without service disruption.

**Note** NAI support in Mobile IP HA Redundancy feature provides capabilities specific to CDMA2000 for Home Agent redundancy. The CDMA2000 framework requires address assignment based on NAI, and support of multiple static IP addresses per user NAI.

The Home Agent Redundancy feature is supported for Static IP Address assignment and IP Address assignment by AAA. Starting in Release 2.0, the Home Agent Redundancy feature is supported for Dynamic IP Address assignment using local IP address pools and Dynamic IP Address assignment using Proxy DHCP.

When Home Agent Redundancy is configured with Dynamic IP Address assignment using Proxy DHCP, the DHCP information is not synced with the standby while the bindings are brought up, even though the bindings are synced to the standby HA. However, when the standby HA becomes active, a DHCP request for each existing binding is sent out to the DHCP server in order to update the DHCP related information on this Home Agent.

The following features are not supported with HA redundancy:

- Hot-lining support on HA
- ODAP/DHCP and local pool addressing schemes are not supported with peer-peer redundancy

During the Mobile IP registration process, an HA creates a mobility binding table that maps the home IP address of an MN to the current care-of address of the MN. If the HA fails, the mobility binding table is lost and all MNs registered with the HA lose connectivity. To reduce the impact of an HA failure, Cisco IOS software supports the HA redundancy feature.

**Note** On configurations based on Cisco 7600 series or Catalyst 6500 series platforms, the backup Home Agent image is configured on a different MWAM card from the primary.

The functionality of HA Redundancy runs on top of the Hot Standby Router Protocol (HSRP). HSRP is a protocol developed by Cisco that provides network redundancy in a way that ensures that user traffic immediately and transparently recovers from failures.

## Geographical Redundancy

Home Agents in a redundant pair can be placed at geographically separate locations using a VPN solution (such as one based on MPLS) instead of a LAN/VLAN between Home Agent pairs. Such a deployment needs to implement correct routing logic in the network to route traffic to one of the Home Agents in the pair. If there is a network failure, both of the HAs could transition to HSRP active state. The Home Agent Redundancy feature recovers from this type of failure gracefully with minimal loss of bindings. The following scenario describes the failure recovery process:

1. HA1 (high priority) and HA2 (low priority) are deployed in redundant mode over a WAN link. HSRP is running between the home agents over the WAN link.
2. HA1 is active and HA2 is standby.
3. WAN connectivity to HA1 is lost due to a network fault, so the HSRP link between HA1 and HA2 is lost.
4. HA2 does not receive hello packets, and transitions to active. HA1 remains active as well, for the same reason (the box itself is functional). If this feature is enabled, both HA1 and HA2 lower their priority.
5. Mobile traffic and signaling messages are routed to HA2. HA2 updates its binding table accordingly, and if the feature is enabled, increases its priority back to the original value. But, the changed home agent state information on HA2 does not get synched to HA1 (which is unreachable).
6. Network fault is corrected, and hello packets are exchanged between HA1 and HA2.
7. Without this feature, HA1 remains active and HA2 moves to become standby, leading to loss of latest state information as created on HA2 at Step #5. If this feature is enabled, HA1 moves to become standby and HA2 remains active, and the latest information on HA2 gets synched to HA1. Once state information is replicated, HA1 moves back to its normal priority. This allows HA1 to become active and HA2 to become the standby.

As described above, the latest state information is maintained after network fault is corrected. To enable this feature, issue the following commands on the HA:

**track** *tracking object id* **application home-agent**

This command creates a tracking object to track the home-agent state.

**standby track** *tracking object id* **decrement** *priority*

This command enables lowering priority as required by step #4 in the above failure scenario.

**Note** If preemption is configured, the *priority* value should be greater than the difference in priorities of the active and standby Home Agents.

## Redundancy with Radius Downloaded Pool Names

The Cisco Mobile Wireless Home Agent supports AAA downloadable pool names for address allocation. The radius pool-name attributes returned in an access accept for address allocation are “ip-pool” for dynamic address allocation, and “static-ip-pool” for static address authorization. The pool name returned in an access accept to the Home Agent will be synched to standby Home Agent during normal and bulk sync operation. This enables address allocation from the same pool on the standby Home Agent as well.

## HSRP Groups

Before configuring HA Redundancy, you must understand the concept of HSRP groups.

An HSRP group is composed of two or more routers that share an IP address and a MAC (Layer 2) address, and act as a single virtual router. For example, your Mobile IP topology can include one active HA and one or more standby HAs that the rest of the topology view as a single virtual HA.

You must define certain HSRP group attributes on the interfaces of the HAs so that Mobile IP can implement the redundancy. You can use the groups to provide redundancy for MNs with a home link on either the interface of the group (a physical network) or on virtual networks. Virtual networks are logical circuits that are programmed and share a common physical infrastructure.

# How HA Redundancy Works

The HA Redundancy feature enables you to configure an active HA and one or more standby HAs. The HAs in a redundancy group may be configured in an active HA-standby HA role if the HAs are supporting physical networks, or in a Peer HA-Peer HA role if they are supporting virtual networks.

In the first case, the active HA assumes the lead HA role, and synchronizes the standby HA. In the case of virtual network support, peer HAs share the lead HA role and “update” each other. The peer HA configuration allows for load balancing of the incoming RRQs, as either HA may receive RRQs. In either scenario, the HAs participating in the redundancy group should be configured similarly. The current support structure is 1 to1 to provide the maximum robustness and transparency in failover.

HA functionality is a service provided by the router and is not interface specific. Therefore, the HA and the MN must agree on which HA interface the MN should send its registration requests and, conversely, on which HA interface the HA should receive the registration requests. This agreement must factor in the following two scenarios:

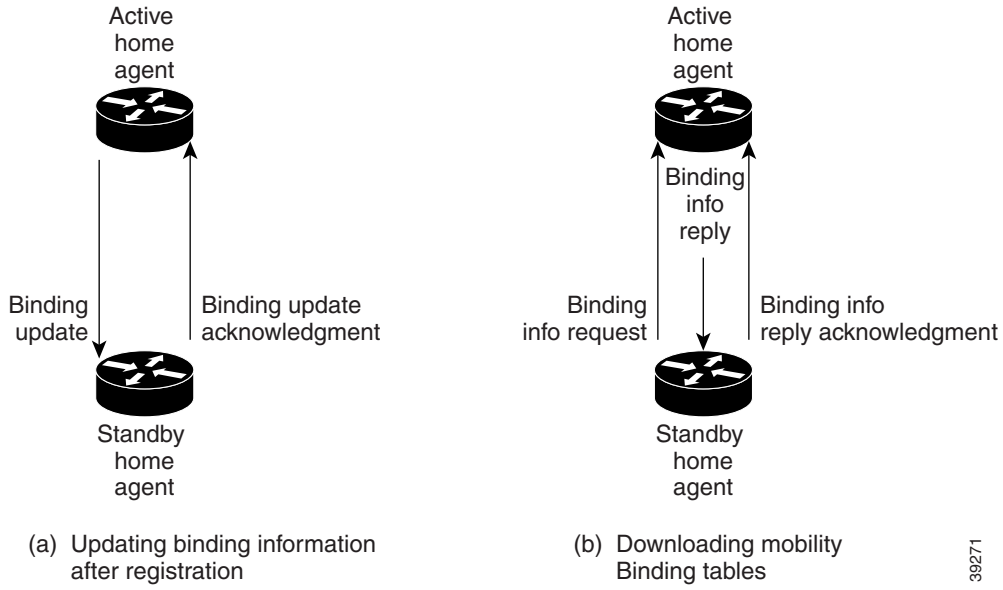
- An MN that has an HA interface (HA IP address) that is not on the same subnet as the MN.
- An MN that requires the HA interface to be on the same subnet as the MN; that is, the HA and the MN must be on the same home network.

For MNs on physical networks, an active HA accepts registration requests from the MN and sends binding updates to the standby HA. This process keeps the mobility binding tables on the active and standby HAs synchronized.

For MNs on virtual networks, the active and standby HAs are peers—either HA can handle registration requests from the MN and update the mobility binding table on the peer HA.

When a standby HA comes up, it must request all mobility binding information from the active HA. The active HA responds by downloading the mobility binding table to the standby HA. The standby HA acknowledges that it has received the requested binding information. Figure 1-1 illustrates an active HA downloading the mobility bindings to a standby HA. A main concern in this stage of the process is which HA IP interface the standby HA should use to retrieve the appropriate mobility binding table, and on which interface of the standby HA the binding request should be sent.

***Figure 1-1 Overview of HA Redundancy and Mobility Binding Process***




**Note** The active HA-standby HA can also be in peer HA-peer HA configuration.

## Physical Network Support

For MNs on physical networks, the HAs are configured in the active HA-standby HA configurations as shown in Figure 1-2 and Figure 1-3. The MNs that are supported on this physical network are configured with the HSRP virtual group address as the HA address. Hence, only the active HA can accept RRQs from the MN because it is the owner of the HSRP virtual group address. Upon receipt of an authenticated RRQ, the active HA sends a binding update to the standby HA.

HA Redundancy for physical networks can support multiple HAs in the redundancy group, although only one HA can be in active state, and only one HA can be in standby state. For example, consider the scenario in which there are four HAs in the redundancy group (that is, one active HA, one standby HA, and two HAs in listen state). If the active HA fails, the standby HA becomes the active HA, and the HA in listen state with higher priority becomes the standby HA.

***Figure 1-2 Virtual Network Support Using One Physical Network (Peer HA-Peer HA)***

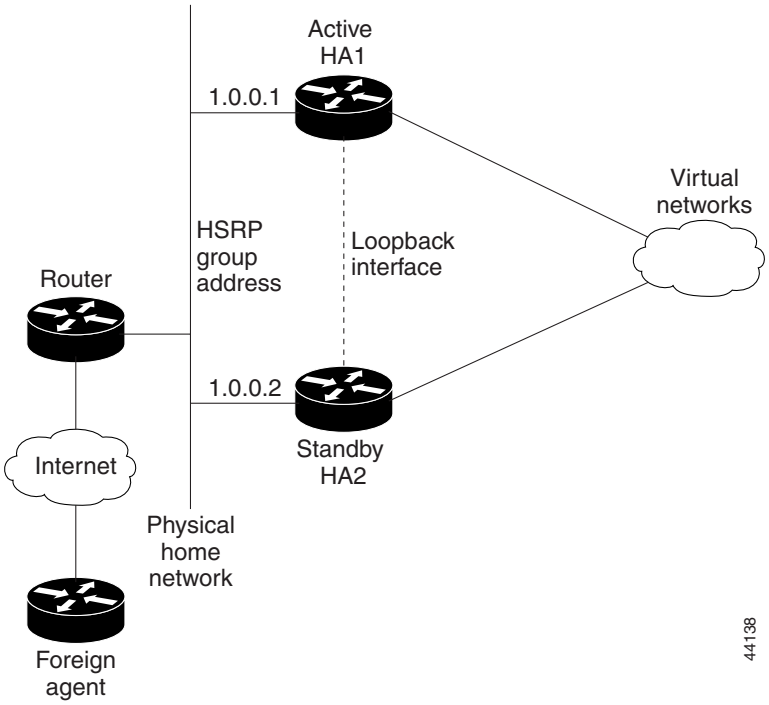
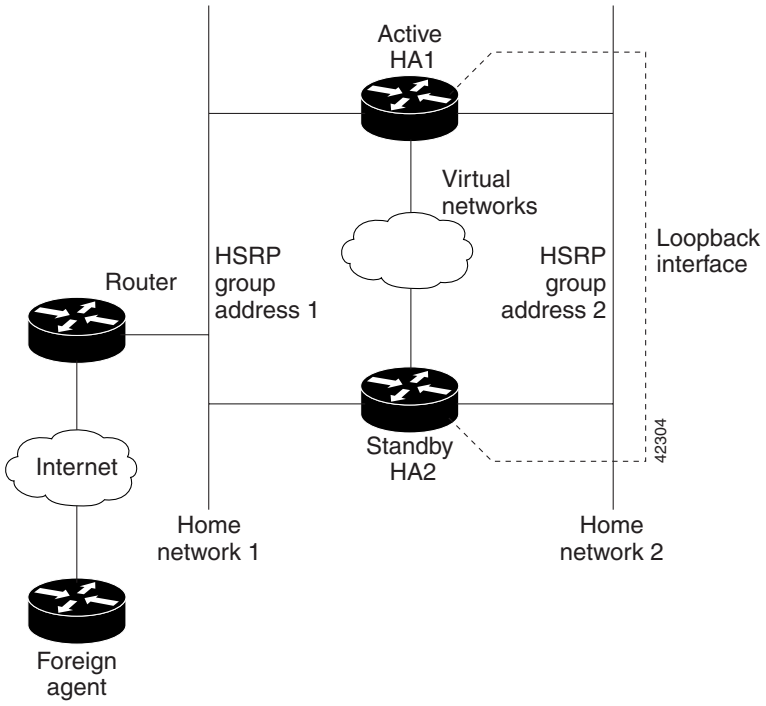


*Figure 1-3 Virtual Network Support Using Multiple Physical Networks (Peer HA-Peer HA)*




# Virtual Networks

Mobile IP calls for each MN are associated with the home network from which the MN's home IP address is allocated. It is often assumed that this should be a physical network, but there are many cases in deployment where it does not make sense to have each MN attached to a physical network. IOS Mobile IP supports the creation of a software interface called a virtual network. A virtual network is very similar to a loopback interface, but it is owned by the Mobile IP process. Using virtual networks saves Interface Descriptor Blocks (IDBs), and allows Mobile IP specific control over how packets are dropped. When using virtual networks the mobile node is always considered roaming, it can never be attached to its home network. In real world deployments, this can cause some semantic problems. For example in cellular deployment a user may be in their home calling area, but will be roaming from a Mobile IP perspective.

Virtual networks are configured and referenced by a network number and mask pair. It is also possible to associate the virtual network with a Home Agent address for redundancy purposes. Here is an example:

```
ip mobile virtual-network 10.0.0.0 255.255.2550.0 address 192.168.100.1
ip mobile host 10.0.0.1 10.0.0.254 virtual-network 10.0.0.0 255.255.255.0
```

Virtual network routes are owned by the Mobile IP routing process and therefore must be redistributed into other routing protocols in order to be propagated. Here is an example:

```
router rip
  redistribute mobile
```

## Support for Discontinuous IP Address Pools for the Same Realm

This feature allows you to specify discontinuous IP address pools for the same realm so that mobiles with NAI can have home addresses assigned from a pool of discontiguous IP address ranges. This will allow the Home Agent to accept Mobiles belonging to multiple virtual networks for the same host group.

To enable this support, configure a local pool on the HA covering the IP address ranges for multiple virtual-networks, and specify one of the virtual-networks as the home network for the given realm.

Use the following configuration to allow the HA to accept MNs belonging to multiple virtual networks for the same host group.

```
ip local pool pool1 10.1.1.1 1.1.1.250
ip local pool pool1 10.1.2.1 1.1.2.250

ip mobile home-agent
ip mobile virtual-network 10.1.1.0 255.255.255.0
ip mobile virtual-network 10.1.2.0 255.255.255.0
ip mobile host nai @xyz.com address pool local pool1 virtual-network 10.1.1.0
255.255.255.0 aaa lifetime 65535
```

In the above configuration, two virtual networks are configured and the local pool (“pool1”) is configured to include the IP addresses for both the virtual networks. By specifying one of the virtual networks and the local pool name in the **ip mobile host** command, the HA accepts MNs belonging to both the networks for the same realm.

# Configuring HA Redundancy

Home Agent Redundancy Tasks (Required for Mobile IP)

To configure your routers for Mobile IP HA redundancy, perform the required tasks described in the following sections:

- Enabling Mobile IP, page 1-7 (Required)
- Enabling HSRP, page 1-8 (Required)
- Configuring HSRP Group Attributes, page 1-8
- Enabling HA Redundancy for a Physical Network, page 1-8 (Required)
- Configuring Geographical Redundancy, page 1-9
- Enabling HA Redundancy for a Virtual Network Using One Physical Network, page 1-9
- Configuring HA Load Balancing, page 1-10

## Enabling Mobile IP

To enable Mobile IP on the router, use the following command in global configuration mode:

| | Command | Purpose |
|---|---|---|
| **Step 1** | Router(config)#router mobile | Enables Mobile IP on the router. |

## Enabling HSRP

To enable HSRP on an interface, use the following command in interface configuration mode:

| | Command | Purpose |
|---|---|---|
| **Step 1** | **Router(config-if)#standby [*group-number*] ip *ip-address*** | Enables HSRP. |

## Configuring HSRP Group Attributes

To configure HSRP group attributes that affect how the local router participates in HSRP, use either of the following commands in interface configuration mode:

| | Command | Purpose |
|---|---|---|
| **Step 1** | Router(config-if)#**standby** [*group-number*] **priority** *priority* [**preempt** [**delay** [**minimum** \| **sync**] *delay*]]<br><br>or<br><br>Router(config-if)#**standby** [*group-number*] [**priority** *priority*] **preempt** [**delay** [**minimum** \| **sync**] *delay*] | Sets the Hot Standby priority used in choosing the active router. By default, the router that comes up later becomes standby. When one router is designated as an active HA, the priority is set highest in the HSRP group and the preemption is set. Configure the **preempt delay min** command so that all bindings will be downloaded to the router before it takes the active role. The router becomes active when all bindings are downloaded, or when the timer expires, whichever comes first. |
| **Step 2** | Router(config-if)# **standby** *group-number* **follow** *group-name* | Specifies the number of the follow group and the name of the primary group to follow and share status.<br><br>We recommend that the specified group number is the same as the primary group number. |

## Enabling HA Redundancy for a Physical Network

To enable HA redundancy for a physical network, use following commands beginning in interface configuration mode:

| | Command | Purpose |
|---|---|---|
| **Step 1** | Router(config-if)#**standby** [*group-number*] **ip** *ip-address* | Enables HSRP. |
| **Step 2** | **Router(config-if)# standby name *hsrp-group-name*** | Sets the name of the standby group. |

| | Command | Purpose |
|---|---|---|
| **Step 3** | `Router(config)#`**`ip mobile home-agent redundancy`** *`hsrp-group-name`* | Configures the Home Agent for redundancy using the HSRP group name. |
| **Step 4** | **`Router(config)#ip mobile secure home-agent`** ***`address`*** **`spi`** ***`spi`*** **`key hex`** ***`string`*** | Sets up the Home Agent security association between peer routers. If configured on the active HA, the IP address argument is that of the standby HA. If configured on the standby HA, the IP address *address* argument is that of the active router. Note that a security association needs to be set up between all HAs in the standby group. |

## Configuring Geographical Redundancy

To enable geographical redundancy on the Home Agent, perform the following tasks:

| | Command | Purpose |
|---|---|---|
| **Step 1** | Router(config)# track tracking object id application home-agent | Creates a tracking object to track the home-agent state. |
| **Step 2** | Router(config)# **`standby track`** *`tracking object id`* **`decrement`** *`priority`* | Enables HAs to lower their priority as required in a failure scenario. |

## Enabling HA Redundancy for a Virtual Network Using One Physical Network

To enable HA redundancy for a virtual network and a physical network, use the following commands beginning in interface configuration mode:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Router (config-if)#` **`standby`** [*`group-number`*] **`ip`** *`ip-address`* | Enables HSRP. |
| **Step 2** | `Router(config)#`**`ip mobile home-agent address`** *`address`*<br><br>or<br><br>`Router(config)#`**`ip mobile home-agent`** | Defines a global Home Agent address. In this configuration, the address is the HSRP group address. Enter this command if the mobile node and Home Agent are on different subnets.<br><br>or<br><br>Enables and controls Home Agent services to the router. Enter this command if the mobile node and Home Agent are on the same subnet. |
| **Step 3** | **`Router(config)#ip mobile virtual-network`** ***`net mask`*** **`[address`** ***`address`*****`]`** | Defines the virtual network. If the mobile node and Home Agent are on the same subnet, use the [**address** *address*] option. |

| | Command | Purpose |
|---|---|---|
| **Step 4** | `Router(config)# ip mobile home-agent redundancy hsrp-group-name [[virtual-network] address address]` | Configures the Home Agent for redundancy using the HSRP group to support virtual networks. |
| **Step 5** | `Router(config)# ip mobile secure home-agent address spi spi key hex string` | Sets up the Home Agent security association between peer routers. If configured on the active HA, the IP address *address* argument is that of the standby HA. If configured on the standby HA, the IP address *address* argument is that of the active router. Note that a security association needs to be set up between all HAs in the standby group. |

## Configuring HA Load Balancing

To enable the HA Load Balancing feature, perform these tasks:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Router(config)# ip mobile home-agent dynamic-address ip address` | Sets the Home Agent Address field in the Registration Response packet. The Home Agent Address field will be set to *ip address*. |

# Home Agent Redundancy Configuration Examples

**Active-HA configuration**

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mwt10-7206b
!
aaa new-model
!
aaa authentication ppp default local group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa session-id common
!
ip subnet-zero
ip cef
!
interface Ethernet2/0
 description to PDSN/FA
 ip address 10.0.0.2 255.0.0.0
 no ip route-cache
 no ip mroute-cache
 duplex half
 standby ip 10.0.0.4
 standby priority 110
 standby preempt delay min 100
 standby name cisco
!
```

```
interface Ethernet2/2
 description to AAA
 ip address 172.16.1.8 255.255.0.0
 no ip route-cache
 no ip mroute-cache
 duplex half
!
router mobile
!
ip local pool ha-pool 10.0.0.1 10.0.0.255
ip classless
no ip http server
ip pim bidir-enable
ip mobile home-agent
ip mobile home-agent redundancy cisco
ip mobile host nai mwts-mip-np-user1@ispxyz.com static-address 40.0.0.1 interface
Ethernet2/0 aaa
ip mobile secure home-agent 7.0.0.3 spi 100 key ascii redundancy algorithm md5 mode
prefix-suffix
!
radius-server host 172.16.0.2 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
gatekeeper
 shutdown
!
line con 0
line aux 0
line vty 0 4
!
end
```

### Standby-HA configuration

```
~~~~~~~~~~~~~~~~~~~~
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mwt10-7206b
!
aaa new-model
!
aaa authentication ppp default local group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa session-id common
!
ip subnet-zero
ip cef
!
interface Ethernet2/0
 description to PDSN/FA
```

```
 ip address 10.0.0.3 255.0.0.0
 no ip route-cache
 no ip mroute-cache
 duplex half
 standby ip 10.0.0.4
 standby name cisco
!
interface Ethernet2/2
 description to AAA
 ip address 172.16.1.7 255.255.0.0
 no ip route-cache
 no ip mroute-cache
 duplex half
!
router mobile
!
ip local pool ha-pool 10.0.0.1 10.0.0.255
ip classless
no ip http server
ip pim bidir-enable
ip mobile home-agent
ip mobile home-agent redundancy cisco
ip mobile host nai mwts-mip-np-user1@ispxyz.com static-address 40.0.0.1 interface
Ethernet2/0 aaa
ip mobile secure home-agent 10.0.0.2 spi 100 key ascii redundancy algorithm md5 mode
prefix-suffix
!
radius-server host 172.16.0.2 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
gatekeeper
 shutdown
!
line con 0
line aux 0
line vty 0 4
!
end
```

CHAPTER 1

# Configuring Load Balancing on the Home Agent

This chapter discusses concepts and configuration details regarding Server Load Balancing on the Cisco Mobile Wireless Home Agent.

This chapter includes the following sections:



## HA Server Load Balancing

The HA-Server Load Balancing (HA-SLB) feature is built upon the existing IOS Server Load Balancing (SLB) feature. SLB allows users to represent a group of network servers (a server farm) as a single server instance, balance the traffic to the servers, and limit traffic to individual servers. The single server instance that represents a server farm is referred to as a virtual server. The servers that comprise the server farm are referred to as real servers.

SLB can distribute the traffic to real servers through mechanisms like round robin to real servers. Additionally, it can monitor the health of each real server using the Dynamic Feedback Protocol, choose a server that has the least load, and choose a server that is up and running. Please refer to the following URL for more information on SLB architecture:

http://www.cisco.com/en/US/products/hw/routers/ps341/products_white_paper09186a0080108939.shtml.

The HA-SLB feature is available on the 6500 and 7600 series platforms. This feature allows a set of real Home Agents, each running on an MWAM, to be identified by a single virtual server IP address residing on 6500 and 7600 Supervisor.

PDSN/FAs send an initial registration request for a user to the virtual server IP address. HA-SLB running on the SUP intercepts the packets and forwards the registration request to one of the real Home Agents.

A typical call flow would have the following sequence of events:

**Step 1** PDSN/FA forwards a Mobile IP RRQ to virtual server IP address (HA-SLB). If the AAA server returns the HA address to the PDSN/FA, the AAA server must be configured to return the address of virtual server IP address.

**Step 2** SLB picks one of the real server/HAs from its serverfarm and it delivers Mobile IP RRQ to this server.

**Step 3** The real HA responds to MobileIP RRQ with a Reply, the message is sent from the real HA to the PDSN/FA. The HA-SLB does not intercept this packet. The real HA creates a binding and local tunnel endpoint.

**Step 4** The PDSN/FA creates a visitor table entry and local tunnel endpoint, and sends/receives traffic through the tunnel directly from the real HA

**Step 5** The PDSN/FA sends a Mobile IP RRQ with lifetime of "0" to the real HA to close the binding.

**Note** The packet is not sent to virtual IP address (HA-SLB)

**Step 6** The Real HA sends Mobile IP RRP to PDSN/FA. The HA-SLB does not intercept this packet. Real HA closes the binding.

**Note** The Mobile IP Messages are not compliant with RFC 2002. But they are compliant to draft-kulkarni-mobile-ip-dynamic-ha-assignment-frmwrk-00.txt.

RRQs destined to the HA/SLB virtual IP address, with an HA address of 0.0.0.0 or 255.255.255.255, are forwarded to the actual HA using a weighted "round-robin," load balancing algorithm. The SLB mechanism supports Dynamic Feedback Protocol (DFP) that gives real servers the ability to communicate real server health to the load balancer, thereby adjusting the weight of the reals server in the load balancing algorithms.

Since the MN can send multiple RRQs before it hears a RRP from the HA (either the MN power cycles after sending an initial RRQ, or it is mis-configured to send multiple initial registrations, or RRPs are dropped by the network), it is important to keep track of registrations coming from the same MN. This avoids the case where the same MN is registered at multiple HAs, and wastes IP addresses and other resources at those HAs. To solve this problem, HA-SLB would parse the RRQ and create a session object indexed by the MNs NAI. This session object will store the real HA IP address where the RRQ was forwarded. Subsequent registrations from the same MN will be forwarded to this same real HA. The session object will be stored for a configurable period of time (default to 10 seconds). If the HA-SLB does not see a RRQ from the MN within this period of time, the session object is cleared. If HA-SLB sees a RRQ, the timer associated with the session object is reset.

A retry counter is associated with each session object, and is incremented for each re-transmitted RRQ seen by the load balancer. If the number of retries is greater than the configured "reassign" threshold, the session sending the retransmissions will be re-assigned to another real HA, and a connection failure is recorded for the original real HA. Real servers are assumed to be down and no more RRQs re-directed to them when enough connection failures are seen to reach a configured threshold. HA-SLB will restart directing sessions to that real server after a configurable time interval or if the real server sends a DFP message to HA-SLB.

## Load Balancing in HA-SLB

HA-SLB uses a weighted round-robin load-balancing algorithm. This algorithm specifies that the real server used for a new connection to the virtual server is chosen from the server farm in a circular fashion. Each real server is assigned a weight *n*, that represents its capacity to handle connections, as compared to the other real servers associated with the virtual server. As an example, assume a server farm comprised of real server ServerA with n = 3, ServerB with n = 1, and ServerC with n = 2. The first three RRQs to the virtual server are assigned to ServerA, the fourth RRQ to ServerB, and the fifth and sixth RRQs to ServerC.

It is possible to configure IOS SLB for either static or dynamic load balancing. Static load balancing is achieved by assigning weights statically to each HA in the server farm. Dynamic load balancing is achieved by configuring Dynamic Feedback Protocol (DFP), with the DFP manager on SLB, and the DFP client on each of the real HAs.

## HA-SLB Operating Modes

HA-SLB operates in two modes, Dispatched mode and Direct (NAT server) mode.

In Dispatched mode the virtual server address is known to the HAs. HA-SLB will simply redirect packets to the HAs at the MAC layer. This requires the HAs to be layer 2 adjacent to SLB.

In Direct mode, HA-SLB works in NAT server mode and routes the RRQs to the HAs by changing the destination IP address in the RRQ to that of the real server. As a result the HAs need not be layer 2 adjacent to SLB.

To configure your routers for Mobile IP HA redundancy, perform the required tasks described in the following sections:

- Configuring HA Load Balancing, page 1-3
- Configuring Server Load Balancing, page 1-3

## Configuring HA Load Balancing

To enable the HA Load Balancing feature, perform these tasks:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Router(config)# ip mobile home-agent dynamic-address` *ip address* | Sets the Home Agent Address field in the Registration Response packet. The Home Agent Address field will be set to *ip address*. |

## Configuring Server Load Balancing

To enable the Mobile IP SLB feature on the HA, perform the following task:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Router(config)# virtual` *ip address* `udp 434 service ipmobile` | Enables the Mobile IP SLB feature. The *ip address* is the virtual Home Agent address to which registration requests from PDSN/FA will be sent. |

# HA-SLB Configuration Examples

The following examples illustrate various HA-SLB configurations, including how to verify details of the configurations.

## Dispatched MODE WITH STATIC WEIGHTS

### Configuration on SLB:

The following commands configure a serverfarm "HAFARM", and associate two real servers (HAs) with the serverfarm. The real servers are configured with a static weight of one.

```
ip slb serverfarm HAFARM
 real 10.1.1.51
  weight 1
  inservice
 !
 real 10.1.1.52
  weight 1
  inservice
```

The following commands configure a virtual server with service as "ipmobile" on the SLB and associates the serverfarm "HAFARM" with the virtual server. Optionally, the **idle ipmobile request** *idle-time-val* command configures the duration for which the session object exists.

```
ip slb vserver MIPSLB
 virtual 10.1.1.10 udp 434 service ipmobile
 serverfarm HAFARM
 idle ipmobile request 300
 inservice
```

### Configuration on HA:

The following command configures the virtual server address as a loopback address on the HA. This configuration is required only for Dispatched mode.

```
interface Loopback1
ip address 10.1.1.10 255.255.255.0
```

The following command sets the source address and HA address field in the RRP to that of the real HA's address. This configuration is required only for Dispatched mode.

```
ip mobile home-agent dynamic-address 10.1.1.51
```

### Show Output on SLB:

The following command displays the status of server farm "HAFARM" and, the associated real servers, and their status. It also shows the number of connections assigned to each of the real servers.

The show output below was captured after opening 4 MIP sessions which HA-SLB has load balanced equally across two real HA's (2 connections to each HA).

```
SLB-6500#show ip slb reals

real                  farm name        weight  state          conns
--------------------------------------------------------------------
20.1.1.51             HAFARM           1       OPERATIONAL    2
20.1.1.52             HAFARM           1       OPERATIONAL    2
```

The following command displays all the sessions during runtime, or as long as the session objects exist.

```
SLB-6500#show ip slb sessions ipmobile

vserver         NAI hash           client             real                       state
-------------------------------------------------------------------------------------------
-
MIPSLB          A984DF0A00000000 15.1.1.51      20.1.1.52              IPMOBILE_ESTAB
MIPSLB          1DC0E31400000000 15.1.1.51       20.1.1.52              IPMOBILE_ESTAB
MIPSLB          2BDEE91100000000 15.1.1.51       20.1.1.51              IPMOBILE_ESTAB
MIPSLB          47E2FD1B00000000 15.1.1.51       20.1.1.51              IPMOBILE_ESTAB
SLB-6500#
```

#### Show Output on HAs:

The following command shows that two bindings each were opened on HA1 and HA2.

```
HA1-7200#show ip mobile binding summary
Mobility Binding List:
Total 2
HA1-7200#

HA2-7200#show ip mobile binding summary
Mobility Binding List:
Total 2
HA2-7200#
```

### Dispatched mode with DFP

#### Configuration on SLB:

The following commands configure a serverfarm “HAFAR”" and associates two real servers (HAs) with the serverfarm.

```
ip slb serverfarm HAFARM
 real 10.1.1.51
  inservice
 !
 real 10.1.1.52
  inservice
!
```

The following commands configure a virtual server with service as “ipmobile” on the SLB, and associates the serverfam HAFARM with the virtual server. The optional **idle ipmobile request** *idle-time-val* command configures the duration the session object exists.

```
ip slb vserver MIPSLB
 virtual 10.1.1.10 udp 434 service ipmobile
 serverfarm HAFARM
 idle ipmobile request 300
 inservice
```

The following command configures the DFP Manager on HA-SLB and assigns two DFP agents (clients) the HA-SLB can connect to.

```
ip slb dfp
 agent 10.1.1.51 500
 agent 10.1.1.52 500
!
```

**Configuration on HA:**

The following command configures the virtual server address as a loopback address on the HA. This configuration is required for dispatched mode.

```
interface Loopback1
ip address 15.1.1.10 255.255.255.0
!
```

The following command configures the DFP agent on the real HA. The port number configured must match the port number specified on the DFP Manager.

```
ip dfp agent ipmobile
 port 500
 inservice
!
```

The following command sets the source address and HA address field in the RRP to that of the real HA's address. This configuration is required for dispatched mode.

```
ip mobile home-agent dynamic-address 10.1.1.51
```

**Show Output on SLB:**

The following command verifies that the HAs report an initial weight of 25 (default weight) when DFP is configured.

```
SLB-6500#show ip slb dfp weights
   Real IP Address: 10.1.1.51 Protocol: UDP Port: 434 Bind_ID: 65535 Weight: 25
      Set by Agent 10.1.1.51:500 at 14:59:23 UTC 04/21/03
   Real IP Address: 10.1.1.52 Protocol: UDP Port: 434 Bind_ID: 65535 Weight: 25
      Set by Agent 10.1.1.52:500 at 14:59:15 UTC 04/21/03
SLB-6500#
```

The following show command displays the status of server farm HAFARM and the associated real servers (and their status). It also shows the number of connections assigned to each of the real servers.

This show output was captured after opening 100 MIP sessions which HA-SLB has load balanced equally across two real HAs (50 connections to each HA).

```
SLB-6500#show ip slb reals

real                  farm name        weight  state          conns
--------------------------------------------------------------------
10.1.1.51             HAFARM           24      OPERATIONAL    50
10.1.1.52             HAFARM           24      OPERATIONAL    50
SLB-6500#
```

**Show output on HAs:**

The following command verifies that 50 bindings each were opened on HA1 and HA2

```
HA1-7200#show ip mobile binding summary
Mobility Binding List:
Total 50
HA1-7200#

HA2-7200#show ip mobile binding summary
Mobility Binding List:
Total 50
HA2-7200#
```

## Direct Mode With Static Weights

### Configuration on SLB:

The following commands configure a serverfarm "HAFARM" and associates two real servers (HAs) with the serverfarm. The real servers are configured with a static weight of one. The command **nat server** configures HA-SLB in Direct (Nat server) mode of operation.

```
ip slb serverfarm HAFARM
nat server
real 10.1.1.51
  weight 1
  inservice
 !
 real 10.1.1.52
  weight 1
  inservice

ip slb vserver MIPSLB
 virtual 10.1.1.10 udp 434 service ipmobile
 serverfarm HAFARM
 idle ipmobile request 300
 inservice
```

### Show Output on SLB:

The following show command displays the status of server farm HAFARM and the associated real servers (and their status). It also shows the number of connections assigned to each of the real servers.

This show output was captured after opening 4 MIP sessions which HA-SLB has load balanced equally across two real HAs (2 connections to each HA).

```
SLB-6500#show ip slb reals

real                  farm name        weight  state          conns
-------------------------------------------------------------------
10.1.1.51             HAFARM           1       OPERATIONAL    2
10.1.1.52             HAFARM           1       OPERATIONAL    2
```

The following command displays all the sessions during runtime, or as long as the session objects exist.

```
SLB-6500#show ip slb sessions ipmobile

vserver         NAI hash         client          real                  state
-------------------------------------------------------------------------------
MIPSLB          A984DF0A00000000 15.1.1.51       20.1.1.52             IPMOBILE_ESTAB
MIPSLB          1DC0E31400000000 15.1.1.51       20.1.1.52             IPMOBILE_ESTAB
MIPSLB          2BDEE91100000000 15.1.1.51       20.1.1.51             IPMOBILE_ESTAB
MIPSLB          47E2FD1B00000000 15.1.1.51       20.1.1.51             IPMOBILE_ESTAB

SLB-6500#
```

#### Show Output on HAs:

The following command shows that 2 bindings each were opened on HA1 and HA2.

```
HA1-7200#show ip mobile binding summary
Mobility Binding List:
Total 2
HA1-7200#

HA2-7200#show ip mobile binding summary
Mobility Binding List:
Total 2
HA2-7200#
```

The following debug command output shows NAT server mode is operational:

```
SLB-6500#debug ip slb sessions ipmobile
SLB-6500#
*Apr 21 15:25:58: %SYS-5-CONFIG_I: Configured from console by console
*Apr 21 15:26:03: SLB_SESSION_IPMOBILE: client = 15.1.1.51, NAI:
mwts-mip-np-user1@ispxyz.com, length: 28
*Apr 21 15:26:03: SLB_SESSION_IPMOBILE: event= IPMOBILE_REQ_REQUEST, state= IPMOBILE_INIT
-> IPMOBILE_ESTAB
*Apr 21 15:26:03: SLB_SESSION: v_ip= 15.1.1.10:434 (  7), real= 20.1.1.51, NAT= S
*Apr 21 15:26:03: SLB_SESSION: client= 15.1.1.51:434 session_key= 47E2FD1B00000000
SLB-6500#
```

## Direct Mode with DFP

#### Configuration on SLB:

The following commands configure a serverfarm "HAFARM", and associate two real servers (HAs) with the serverfarm. The **nat server** command configures HA-SLB in Direct (Nat server) mode of operation.

```
ip slb serverfarm HAFARM
nat server
real 10.1.1.51
  inservice
 !
 real 10.1.1.52
  weight 1
  inservice
!
```

The following commands configure a virtual server with service as "ipmobile" on the SLB, and associates the serverfarm HAFARM with the virtual server. The optional **idle ipmobile request** *idle-time-val* command configures the duration the session object exists.

```
ip slb vserver MIPSLB
 virtual 10.1.1.10 udp 434 service ipmobile
 serverfarm HAFARM
 idle ipmobile request 300
 inservice
!
```

The following command configures the DFP Manager on HA-SLB and assigns two DFP agents (clients) he HA-SLB can connect to.

```
ip slb dfp
 agent 10.1.1.51 500
 agent 10.1.1.52 500
```

**Configuration on HA:**

The following command configures the DFP agent on the real HA. Configure the port number to match the port number specified on the DFP Manager.

```
ip dfp agent ipmobile
 port 500
 inservice
!
```

**Show Output on SLB:**

The following command verifies that the HAs report an initial weight of 25 (default weight) when DFP is configured.

```
SLB-6500#show ip slb dfp weights
   Real IP Address: 10.1.1.51 Protocol: UDP Port: 434 Bind_ID: 65535 Weight: 25
      Set by Agent 10.1.1.51:500 at 14:59:23 UTC 04/21/03
   Real IP Address: 10.1.1.52 Protocol: UDP Port: 434 Bind_ID: 65535 Weight: 25
      Set by Agent 10.1.1.52:500 at 14:59:15 UTC 04/21/03
SLB-6500#
```

The following show command displays the status of server farm “HAFARM”, the associated real servers (and their status). It also shows the number of connections assigned to each of the real servers.

This show output below was captured after opening 100 MIP sessions which HA-SLB has load balanced equally across two real HAs (50 connections to each HA).

```
SLB-6500#show ip slb reals

real                  farm name        weight  state          conns
-------------------------------------------------------------------
10.1.1.51             HAFARM           24      OPERATIONAL    50
10.1.1.52             HAFARM           24      OPERATIONAL    50
SLB-6500#
```

**Show Output on HAs:**

The following command shows that 50 bindings each were opened on HA1 and HA2.

```
HA1-7200#show ip mobile binding summary
Mobility Binding List:
Total 50
HA1-7200#

HA2-7200#show ip mobile binding summary
Mobility Binding List:
Total 50
HA2-7200#
```

The following debug when enabled shows NAT server mode is operational:

```
SLB-6500#debug ip slb sessions ipmobile
SLB-6500#
*Apr 21 15:47:16: SLB_SESSION_IPMOBILE: client = 10.1.1.51, NAI:
mwts-mip-np-user1@ispxyz.com, length: 28
*Apr 21 15:47:16: SLB_SESSION_IPMOBILE: event= IPMOBILE_REQ_REQUEST, state= IPMOBILE_INIT
-> IPMOBILE_ESTAB
*Apr 21 15:47:16: SLB_SESSION: v_ip= 10.1.1.10:434 (  7), real= 20.1.1.51, NAT= S
*Apr 21 15:47:16: SLB_SESSION: client= 10.1.1.51:434 session_key= 47E2FD1B00000000
*Apr 21 15:47:16: SLB_SESSION_IPMOBILE: client = 15.1.1.51, NAI:
mwts-mip-np-user2@ispxyz.com, length: 28
*Apr 21 15:47:16: SLB_SESSION_IPMOBILE: event= IPMOBILE_REQ_REQUEST, state= IPMOBILE_INIT
-> IPMOBILE_ESTAB
*Apr 21 15:47:16: SLB_SESSION: v_ip= 10.1.1.10:434 (  7), real= 20.1.1.51, NAT= S
*Apr 21 15:47:16: SLB_SESSION: client= 10.1.1.51:434 session_key= 1DC0E31400000000
```

## Dispatched Mode of Operation and Crypto Transform Mode is Tunnel

The following command verifies the status of the IPSEC VPN module:

```
SLB1-6500#show module
Mod Ports Card Type                                Model              Serial No.
--- ----- ---------------------------------------- ------------------ -----------
  1    2  Catalyst 6000 supervisor 2 (Active)    WS-X6K-S2U-MSFC2   SAD070701KR
  3   48  SFM-capable 48-port 10/100 Mbps RJ45   WS-X6548-RJ-45     SAL0706CVFQ
  5    3  MWAM Module                            WS-SVC-MWAM-1      SAD06420188
  6    2  IPSec VPN Accelerator                  WS-SVC-IPSEC-1     SAD064902NT

Mod MAC addresses                       Hw    Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
  1  0001.6416.4ffe to 0001.6416.4fff   4.2   6.1(3)       7.5(0.94)    Ok
  3  0009.11f4.9b60 to 0009.11f4.9b8f   5.2   6.3(1)       7.5(0.94)    Ok
  5  0008.7ca8.17d8 to 0008.7ca8.17df   0.302 7.2(1)       1.0(0.1)     Ok
  6  0002.7ee4.c34e to 0002.7ee4.c351   1.0   7.2(1)       7.5(0.94)    Ok

Mod Sub-Module                  Model           Serial          Hw     Status
--- --------------------------- --------------- --------------- ------- -------
  1 Policy Feature Card 2       WS-F6K-PFC2     SAD07060047     3.3    Ok
  1 Cat6k MSFC 2 daughterboard  WS-F6K-MSFC2    SAD070701FS     2.5    Ok

Mod Online Diag Status
--- -------------------
  1 Pass
  3 Pass
  5 Pass
  6 Pass
SLB1-6500#
```

### Configuration on SLB:

```
ip slb serverfarm FARM1
 real 10.99.11.11
  inservice
 !
 real 10.99.11.12
  inservice
!
ip slb vserver IPSECSLB
 virtual 10.1.1.10 udp 434 service ipmobile
 serverfarm FARM1
 inservice
```

The following commands configure IPSEC on HA-SLB:

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 10.1.1.51
!
!
crypto ipsec transform-set esp-des-sha-transport ah-sha-hmac esp-des
!
crypto map l2tpmap 10 ipsec-isakmp
 set peer 10.1.1.51
 set transform-set esp-des-sha-transport
 match address 101
!
interface GigabitEthernet6/1 (inside port of the IPSEC module)
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,15,1002-1005
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet6/2       (outside port of the IPSEC module)
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,16,1002-1005
 switchport mode trunk
 cdp enable
!
interface FastEthernet3/15
 no ip address
 duplex full
 speed 100
 crypto connect vlan 15
!
!
interface Vlan15
 ip address 10.1.1.15 255.0.0.0
 no ip redirects
 no ip unreachables
 no mop enabled
 crypto map l2tpmap
!
!
access-list 101 permit ip host 10.1.1.10 host 10.1.1.51
```

**Configuration on PDSN:**

The following commands configure IPSEC on PDSN:

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 10.1.1.15
!
!
crypto ipsec transform-set esp-des-sha-transport esp-des esp-sha-hmac
!
crypto map l2tpmap 10 ipsec-isakmp
 set peer 10.1.1.15
 set transform-set esp-des-sha-transport
 match address 101

interface FastEthernet1/0
 ip address 10.1.1.51 255.0.0.0
```

```
 duplex full
 crypto map l2tpmap

access-list 101 permit ip host 15.1.1.51 host 15.1.1.10
```

#### Configuration on HA:

```
interface Loopback1
 ip address 10.1.1.10 255.0.0.0

ip mobile home-agent dynamic-address 10.99.11.11
```

Execute the **clear crypto isakmp** and **clear crypto sa** commands on the PDSN and SLB, and open multiple MIP flows.

#### Show Output on PDSN (FA):

The following command verifies that packets sent out of the PDSN are encrypted:

```
PDSN-7200#show crypto ipsec sa

interface: FastEthernet1/0
    Crypto map tag: l2tpmap, local addr. 10.1.1.51

   local  ident (addr/mask/prot/port): (10.1.1.51/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.10/255.255.255.255/0/0)
   current_peer: 10.1.1.15
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 16, #recv errors 0

     local crypto endpt.: 10.1.1.51, remote crypto endpt.: 10.1.1.15
     path mtu 1500, media mtu 1500
     current outbound spi: FD2E19D2


     inbound esp sas:
      spi: 0x2AEF7930(720337200)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2002, flow_id: 1, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3454)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:
      spi: 0xE12F5466(3777975398)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3454)
        replay detection support: Y

     inbound pcp sas:

     outbound esp sas:
      spi: 0xFD2E19D2(4247656914)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2003, flow_id: 2, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4607999/3454)
```

```
        IV size: 8 bytes
        replay detection support: Y

      outbound ah sas:
       spi: 0x87E60F74(2280001396)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4607999/3445)
        replay detection support: Y

      outbound pcp sas:


PDSN-7200#
```

**Show Output on SLB:**

```
SLB1-6500#sh ip slb reals

real                  farm name        weight  state          conns
--------------------------------------------------------------------
10.99.11.11           FARM1            1       OPERATIONAL    2
10.99.11.12           FARM1            1       OPERATIONAL    2


SLB1-6500#sh ip slb sessions ipmobile

vserver         NAI hash         client          real                    state
-------------------------------------------------------------------------------
IPSECSLB        A984DF0A00000000 10.1.1.51       10.99.11.12             IPMOBILE_ESTAB
IPSECSLB        1DC0E31400000000 10.1.1.51       10.99.11.12             IPMOBILE_ESTAB
IPSECSLB        2BDEE91100000000 10.1.1.51       10.99.11.11             IPMOBILE_ESTAB
IPSECSLB        47E2FD1B00000000 10.1.1.51       10.99.11.11             IPMOBILE_ESTAB
SLB1-6500#
```

The following command verifies that packets received by the HA-SLB are decrypted:

```
SLB1-6500#show crypto ipsec sa

interface: Vlan15
    Crypto map tag: l2tpmap, local addr. 15.1.1.15

   local  ident (addr/mask/prot/port): (10.1.1.10/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.51/255.255.255.255/0/0)
   current_peer: 10.1.1.51
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.1.1.15, remote crypto endpt.: 10.1.1.51
     path mtu 1500, media mtu 1500
     current outbound spi: 2AEF7930

     inbound esp sas:
      spi: 0xFD2E19D2(4247656914)
        transform: esp-des ,
        in use settings ={Tunnel, }
```

```
        slot: 0, conn id: 10999, flow_id: 49, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4607999/3488)
        IV size: 8 bytes
        replay detection support: Y

      inbound ah sas:
       spi: 0x87E60F74(2280001396)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 10997, flow_id: 49, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4607999/3488)
        replay detection support: Y

      inbound pcp sas:

      outbound esp sas:
       spi: 0x2AEF7930(720337200)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 11000, flow_id: 50, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3488)
        IV size: 8 bytes
        replay detection support: Y

      outbound ah sas:
       spi: 0xE12F5466(3777975398)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 10998, flow_id: 50, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3488)
        replay detection support: Y

      outbound pcp sas:


SLB1-6500#
```

### Show Output on HAs:

```
HA1-7200#show ip mobile binding summary
Mobility Binding List:
Total 2
HA1-7200#

HA2-7200#show ip mobile binding summary
Mobility Binding List:
Total 2
HA2-7200#
```

## Dispatched Mode of Operation and Crypto Transform Mode is Transport

### Configuration on SLB:

```
ip slb serverfarm FARM1
 real 10.99.11.11
  inservice
 !
 real 10.99.11.12
  inservice
!
ip slb vserver IPSECSLB
 virtual 10.1.1.10 udp 434 service ipmobile
 serverfarm FARM1
 inservice
```

The following commands configure IPSEC on HA-SLB:

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 10.1.1.51
!
!
crypto ipsec transform-set esp-des-sha-transport ah-sha-hmac esp-des
 mode transport        (The crypto mode is configured as transport )
!
crypto map l2tpmap 10 ipsec-isakmp
 set peer 15.1.1.51
 set transform-set esp-des-sha-transport
 match address 101
!
interface GigabitEthernet6/1 (inside port of the IPSEC module)
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,15,1002-1005
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet6/2       (outside port of the IPSEC module)
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,16,1002-1005
 switchport mode trunk
 cdp enable
!
interface FastEthernet3/15
 no ip address
 duplex full
 speed 100
 crypto connect vlan 15
!
!
interface Vlan15
 ip address 10.1.1.15 255.0.0.0
 no ip redirects
 no ip unreachables
 no mop enabled
 crypto map l2tpmap
!
!
access-list 101 permit ip host 10.1.1.10 host 10.1.1.51
```

**Configuration on PDSN:**

The following commands configure IPSEC on PDSN:

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 10.1.1.15
!
!
crypto ipsec transform-set esp-des-sha-transport esp-des esp-sha-hmac
 mode transport        (The crypto mode is configured as transport )
!
crypto map l2tpmap 10 ipsec-isakmp
 set peer 10.1.1.15
 set transform-set esp-des-sha-transport
 match address 101

interface FastEthernet1/0
 ip address 10.1.1.51 255.0.0.0
 duplex full
 crypto map l2tpmap

access-list 101 permit ip host 10.1.1.51 host 10.1.1.10
```

**Configuration on HA:**

```
interface Loopback1
 ip address 10.1.1.10 255.0.0.0

ip mobile home-agent dynamic-address 10.99.11.11
```

Execute the **clear crypto isakmp** and **clear crypto sa** commands on the PDSN and SLB, and open multiple MIP flows.

**Show Output on PDSN :**

The following command verifies that packets sent out of the PDSN are encrypted:

```
PDSN-7200#sh crypto ipsec sa

interface: FastEthernet1/0
    Crypto map tag: l2tpmap, local addr. 10.1.1.51

   local  ident (addr/mask/prot/port): (10.1.1.51/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.10/255.255.255.255/0/0)
   current_peer: 10.1.1.15
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 4, #recv errors 0

     local crypto endpt.: 10.1.1.51, remote crypto endpt.: 10.1.1.15
     path mtu 1500, media mtu 1500
     current outbound spi: 9DB2749C

     inbound esp sas:
      spi: 0x29960A54(697698900)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2002, flow_id: 1, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3536)
```

```
      IV size: 8 bytes
      replay detection support: Y

    inbound ah sas:
     spi: 0x4CB25D79(1286757753)
      transform: ah-sha-hmac ,
      in use settings ={Tunnel, }
      slot: 0, conn id: 2000, flow_id: 1, crypto map: l2tpmap
      sa timing: remaining key lifetime (k/sec): (4608000/3527)
      replay detection support: Y

    inbound pcp sas:

    outbound esp sas:
     spi: 0x9DB2749C(2645718172)
      transform: esp-des ,
      in use settings ={Tunnel, }
      slot: 0, conn id: 2003, flow_id: 2, crypto map: l2tpmap
      sa timing: remaining key lifetime (k/sec): (4607999/3527)
      IV size: 8 bytes
      replay detection support: Y

    outbound ah sas:
     spi: 0x3F9BDD27(1067179303)
      transform: ah-sha-hmac ,
      in use settings ={Tunnel, }
      slot: 0, conn id: 2001, flow_id: 2, crypto map: l2tpmap
      sa timing: remaining key lifetime (k/sec): (4607999/3527)
      replay detection support: Y

    outbound pcp sas:


PDSN-7200#
```

### Show Output on SLB:

```
SLB1-6500#sh ip slb sessions ipmobile

vserver         NAI hash         client          real                  state
-------------------------------------------------------------------------------
IPSECSLB        A984DF0A00000000 10.1.1.51       10.99.11.12           IPMOBILE_ESTAB
IPSECSLB        1DC0E31400000000 10.1.1.51       10.99.11.12           IPMOBILE_ESTAB
IPSECSLB        2BDEE91100000000 10.1.1.51       10.99.11.11           IPMOBILE_ESTAB
IPSECSLB        47E2FD1B00000000 10.1.1.51       10.99.11.11           IPMOBILE_ESTAB
SLB1-6500#
SLB1-6500#sh ip sl
SLB1-6500#sh ip slb rea
SLB1-6500#sh ip slb reals

real                 farm name        weight  state          conns
-------------------------------------------------------------------
10.99.11.11          FARM1            1       OPERATIONAL    2
10.99.11.12          FARM1            1       OPERATIONAL    2
SLB1-6500#
```

The following command verifies that packets received by the HA-SLB are decrypted:

```
SLB1-6500#show crypto ipsec sa

interface: Vlan15
    Crypto map tag: l2tpmap, local addr. 10.1.1.15

   local  ident (addr/mask/prot/port): (10.1.1.10/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.51/255.255.255.255/0/0)
   current_peer: 10.1.1.51
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 15.1.1.15, remote crypto endpt.: 10.1.1.51
     path mtu 1500, media mtu 1500
     current outbound spi: 29960A54

     inbound esp sas:
      spi: 0x9DB2749C(2645718172)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 11011, flow_id: 55, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4607999/3540)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:
      spi: 0x3F9BDD27(1067179303)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 11009, flow_id: 55, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4607999/3540)
        replay detection support: Y

     inbound pcp sas:

     outbound esp sas:
      spi: 0x29960A54(697698900)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 11012, flow_id: 56, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3540)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:
      spi: 0x4CB25D79(1286757753)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 11010, flow_id: 56, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3540)
        replay detection support: Y

     outbound pcp sas:


SLB1-6500#
```

### Show Output on HAs:

```
HA5-2#sh ip mob binding summary
Mobility Binding List:
Total 2

HA5-3#sh ip mob binding summary
Mobility Binding List:
Total 2
HA5-3#
```

## Direct Mode of Operation and Crypto Transform Mode is Tunnel

```
Configuration on SLB:
ip slb serverfarm FARM1
 nat server
 real 10.99.11.11
  inservice
 !
 real 10.99.11.12
  inservice
!
ip slb vserver IPSECSLB
 virtual 15.1.1.10 udp 434 service ipmobile
 serverfarm FARM1
 inservice
```

The following commands configure IPSEC on HA-SLB:

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 10.1.1.51
!
!
crypto ipsec transform-set esp-des-sha-transport ah-sha-hmac esp-des
!
crypto map l2tpmap 10 ipsec-isakmp
 set peer 10.1.1.51
 set transform-set esp-des-sha-transport
 match address 101
!
interface GigabitEthernet6/1 (inside port of the IPSEC module)
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,15,1002-1005
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet6/2       (outside port of the IPSEC module)
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,16,1002-1005
 switchport mode trunk
 cdp enable
!
interface FastEthernet3/15
 no ip address
 duplex full
 speed 100
 crypto connect vlan 15
!
```

```
!
interface Vlan15
 ip address 10.1.1.15 255.0.0.0
 no ip redirects
 no ip unreachables
 no mop enabled
 crypto map l2tpmap
!
!
access-list 101 permit ip host 10.1.1.10 host 10.1.1.51
```

#### Configuration on PDSN:

The following commands configure IPSEC on PDSN:

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 10.1.1.15
!
!
crypto ipsec transform-set esp-des-sha-transport esp-des esp-sha-hmac
!
crypto map l2tpmap 10 ipsec-isakmp
 set peer 10.1.1.15
 set transform-set esp-des-sha-transport
 match address 101

interface FastEthernet1/0
 ip address 10.1.1.51 255.0.0.0
 duplex full
 crypto map l2tpmap

access-list 101 permit ip host 10.1.1.51 host 10.1.1.10
```

Execute **clear crypto isakmp** and **clear crypto sa** on the PDSN and SLB. Open multiple MIP flows.

Show Output on PDSN:

The following command verifies that packets sent out of the PDSN are encrypted:

```
PDSN-7200#show crypto ipsec sa

interface: FastEthernet1/0
    Crypto map tag: l2tpmap, local addr. 10.1.1.51

   local  ident (addr/mask/prot/port): (10.1.1.51/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.10/255.255.255.255/0/0)
   current_peer: 10.1.1.15
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 4, #recv errors 0

     local crypto endpt.: 10.1.1.51, remote crypto endpt.: 10.1.1.15
     path mtu 1500, media mtu 1500
     current outbound spi: 1A274E9D
```

```
     inbound esp sas:
      spi: 0xD3D5F08B(3554013323)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2002, flow_id: 1, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3026)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:
      spi: 0x7FEE86C3(2146338499)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3026)
        replay detection support: Y

     inbound pcp sas:

     outbound esp sas:
      spi: 0x1A274E9D(438783645)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2003, flow_id: 2, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4607999/3026)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:
      spi: 0x5F9A83(6265475)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4607999/3026)
        replay detection support: Y

     outbound pcp sas:


PDSN-7200#
```

**Show Output on SLB:**

The following command verifies that packets received by HA-SLB are decrypted:

```
SLB1-6500#show crypto ipsec sa

interface: Vlan15
    Crypto map tag: l2tpmap, local addr. 10.1.1.15

   local  ident (addr/mask/prot/port): (10.1.1.10/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.51/255.255.255.255/0/0)
   current_peer: 15.1.1.51
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 15.1.1.15, remote crypto endpt.: 10.1.1.51
     path mtu 1500, media mtu 1500
     current outbound spi: D6C550E1
```

```
     inbound esp sas:
      spi: 0x267FCD46(645909830)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 11027, flow_id: 63, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4607999/3581)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:
      spi: 0xF779A01E(4151943198)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 11025, flow_id: 63, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4607999/3581)
        replay detection support: Y

     inbound pcp sas:

     outbound esp sas:
      spi: 0xD6C550E1(3603255521)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 11028, flow_id: 64, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3581)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:
      spi: 0x325BEB84(844884868)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 11026, flow_id: 64, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3581)
        replay detection support: Y

     outbound pcp sas:

SLB1-6500#show ip slb sessions ipmobile

vserver         NAI hash         client          real                    state
-------------------------------------------------------------------------------
IPSECSLB        A984DF0A00000000 10.1.1.51       10.99.11.12             IPMOBILE_ESTAB
IPSECSLB        1DC0E31400000000 10.1.1.51       10.99.11.12             IPMOBILE_ESTAB
IPSECSLB        2BDEE91100000000 10.1.1.51       10.99.11.11             IPMOBILE_ESTAB
IPSECSLB        47E2FD1B00000000 10.1.1.51       10.99.11.11             IPMOBILE_ESTAB
SLB1-6500#
SLB1-6500#sh ip slb
SLB1-6500#sh ip slb rea
SLB1-6500#sh ip slb reals

real                  farm name        weight  state          conns
-------------------------------------------------------------------
10.99.11.11           FARM1            1       OPERATIONAL    2
10.99.11.12           FARM1            1       OPERATIONAL    2
SLB1-6500

Show output on SLB:
HA5-2#show ip mob binding summary
Mobility Binding List:
Total 2
HA5-2#
```

```
HA5-3#show ip mob binding summary
Mobility Binding List:
Total 2
HA5-3#
```

#### Debug Output on SLB:

The following debug command shows that NAT server mode is operational:

```
SLB1-6500#debug ip slb sessions ipmobile
*Jul  1 05:25:25.513: SLB_SESSION_IPMOBILE: event= IPMOBILE_TIMEOUT, state= IPMOBILE_ESTAB
-> IPMOBILE_INIT
*Jul  1 05:25:25.513: SLB_SESSION: v_ip= 15.1.1.10:434 (  7), real= 99.99.11.12, NAT= S
*Jul  1 05:25:25.513: SLB_SESSION: client= 15.1.1.51:434 session_key= A984DF0A00000000
*Jul  1 05:25:25.513: SLB_SESSION_IPMOBILE: event= IPMOBILE_TIMEOUT, state= IPMOBILE_ESTAB
-> IPMOBILE_INIT
*Jul  1 05:25:25.513: SLB_SESSION: v_ip= 15.1.1.10:434 (  7), real= 99.99.11.11, NAT= S
*Jul  1 05:25:25.513: SLB_SESSION: client= 15.1.1.51:434 session_key= 2BDEE91100000000
*Jul  1 05:25:25.513: SLB_SESSION_IPMOBILE: event= IPMOBILE_TIMEOUT, state= IPMOBILE_ESTAB
-> IPMOBILE_INIT
```

### Direct Mode of Operation and Crypto Transform Mode is Transport

#### Configuration on SLB:

```
ip slb serverfarm FARM1
 nat server
 real 10.99.11.11
  inservice
 !
 real 10.99.11.12
  inservice
!
ip slb vserver IPSECSLB
 virtual 10.1.1.10 udp 434 service ipmobile
 serverfarm FARM1
 inservice
```

The following commands configure IPSEC on the HA-SLB:

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 10.1.1.51
!
!
crypto ipsec transform-set esp-des-sha-transport ah-sha-hmac esp-des
 mode transport    (The crypto mode is configured as transport )
!
crypto map l2tpmap 10 ipsec-isakmp
 set peer 10.1.1.51
 set transform-set esp-des-sha-transport
 match address 101
!
interface GigabitEthernet6/1 (inside port of the IPSEC module)
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,15,1002-1005
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet6/2       (outside port of the IPSEC module)
```

```
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,16,1002-1005
 switchport mode trunk
 cdp enable
!
interface FastEthernet3/15
 no ip address
 duplex full
 speed 100
 crypto connect vlan 15
!
!
interface Vlan15
 ip address 15.1.1.15 255.0.0.0
 no ip redirects
 no ip unreachables
 no mop enabled
 crypto map l2tpmap
!
!
access-list 101 permit ip host 15.1.1.10 host 15.1.1.51
```

**Configuration on PDSN:**

The following commands configure IPSEC on PDSN:

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 10.1.1.15
!
!
crypto ipsec transform-set esp-des-sha-transport esp-des esp-sha-hmac
 mode transport           (The crypto mode is configured as transport )
!
crypto map l2tpmap 10 ipsec-isakmp
 set peer 10.1.1.15
 set transform-set esp-des-sha-transport
 match address 101

interface FastEthernet1/0
 ip address 10.1.1.51 255.0.0.0
 duplex full
 crypto map l2tpmap

access-list 101 permit ip host 15.1.1.51 host 15.1.1.10
```

Execute **clear crypto isakmp** and **clear crypto sa** on the PDSN and SLB. Open multiple MIP flows.

**Show Output on PDSN :**

The following command verifies that packets sent out of the PDSN are encrypted:

```
PDSN-7200#show crypto ipsec sa

interface: FastEthernet1/0
    Crypto map tag: l2tpmap, local addr. 10.1.1.51

   local  ident (addr/mask/prot/port): (10.1.1.51/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.10/255.255.255.255/0/0)
   current_peer: 10.1.1.15
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
```

```
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 4, #recv errors 0

     local crypto endpt.: 10.1.1.51, remote crypto endpt.: 10.1.1.15
     path mtu 1500, media mtu 1500
     current outbound spi: 6A0EBD82

     inbound esp sas:
      spi: 0x13E0E556(333505878)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2002, flow_id: 1, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3535)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:
      spi: 0xEFEEE153(4025409875)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3535)
        replay detection support: Y

     inbound pcp sas:

     outbound esp sas:
      spi: 0x6A0EBD82(1779350914)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2003, flow_id: 2, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4607999/3535)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:
      spi: 0x49BE92A3(1237226147)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4607999/3535)
        replay detection support: Y

     outbound pcp sas:


PDSN-7200#
```

### Show Output on SLB:

```
SLB1-6500#show ip slb sessions ipmobile

vserver         NAI hash         client          real                    state
-------------------------------------------------------------------------------
IPSECSLB        A984DF0A00000000 10.1.1.51       99.99.11.12             IPMOBILE_ESTAB
IPSECSLB        1DC0E31400000000 10.1.1.51       99.99.11.12             IPMOBILE_ESTAB
IPSECSLB        2BDEE91100000000 10.1.1.51       99.99.11.11             IPMOBILE_ESTAB
IPSECSLB        47E2FD1B00000000 10.1.1.51       99.99.11.11             IPMOBILE_ESTAB
SLB1-6500#
SLB1-6500#sh ip slb rea
SLB1-6500#sh ip slb reals
```

```
real                  farm name        weight  state          conns
-------------------------------------------------------------------
99.99.11.11           FARM1            1       OPERATIONAL    2
99.99.11.12           FARM1            1       OPERATIONAL    2
SLB1-6500#
SLB1-6500#
```

The following command verifies that packets received by the HA-SLB are decrypted:

```
SLB1-6500#show crypto ipsec sa

interface: Vlan15
    Crypto map tag: l2tpmap, local addr. 10.1.1.15

   local  ident (addr/mask/prot/port): (10.1.1.10/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.51/255.255.255.255/0/0)
   current_peer: 10.1.1.51
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 15.1.1.15, remote crypto endpt.: 15.1.1.51
     path mtu 1500, media mtu 1500
     current outbound spi: 13E0E556

     inbound esp sas:
      spi: 0x6A0EBD82(1779350914)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 11031, flow_id: 65, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4607999/3527)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:
      spi: 0x49BE92A3(1237226147)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 11029, flow_id: 65, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4607999/3527)
        replay detection support: Y

     inbound pcp sas:

     outbound esp sas:
      spi: 0x13E0E556(333505878)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 11032, flow_id: 66, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3527)
        IV size: 8 bytes
        replay detection support: Y
```

```
     outbound ah sas:
      spi: 0xEFEEE153(4025409875)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 11030, flow_id: 66, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3524)
        replay detection support: Y

     outbound pcp sas:


SLB1-6500#
```

### Show Output on HA:

```
HA5-2#show ip mob binding summary
Mobility Binding List:
Total 2
HA5-2#


HA5-3#show ip mob binding summary
Mobility Binding List:
Total 2
HA5-3#
```

CHAPTER 1

# Terminating IP Registrations

This chapter discusses how the Cisco Mobile Wireless Home Agent terminates IP registrations and how to configure the Home Agent to perform this function.

This chapter includes the following sections:



## Mobile IPv4 Registration Revocation

Basic Mobile IP resource revocation is an IS-835-C initiative that defines the methods by which a mobility agent (one that provides Mobile IP services to a mobile node) can notify the other mobility agent of the termination of a registration due to administrative reasons or MIP handoff.

This feature is similar to the Cisco MobileIP Bind Update feature. When a mobile changes its point of attachment (FA), or needs to terminate the session administratively, the HA sends a registration revocation message to the old FA. The old FA tears down the session and sends a registration revocation acknowledgement message to the HA. Additionally, if the PDSN/FA needs to terminate the session administratively, the FA sends a registration revocation message to the HA. The HA deletes the binding for the mobile, and sends a registration revocation acknowledgement to FA.

An HA configured to support registration revocation in Mobile IPv4 includes a revocation support extension in all MIP RRP for the associated MIP RRQ from the PDSN that contained a valid registration revocation extension. A registration for which the HA received a revocation support extension, and responded with a subsequent revocation support extension, is considered revocable by the HA.

The following sample call flow illustrates Mobile IP Resource Revocation (Registration phase):

**Step 1** The MS originates a call and PPP session is up.

**Step 2** The PDSN/FA has been configured to advertise MIPv4 registration revocation support. The PDSN/FA sends advertisement with MIPv4 Registration revocation support bit “X” set.

**Step 3** The PDSN/FA receives MIP RRQ from MN, includes STC attribute set to **2** in access-request during FA-CHAP. While forwarding the RRQ to the HA, the revocation support extension is appended after the MHAE. The I-bit in the revocation support extension will be set to **1** indicating that the MS would get an explicit notification on revocation of the binding whenever necessary.

**Step 4** The HA, upon receiving the MIP RRQ containing a revocation extension, will send back the MIP RRP including a revocation support extension and setting the I-bit equal to the value received in the MIP RRQ. In case of HA-CHAP (MN-AAA authentication), the STC attribute, with a value of **2**, will be included in the access-request sent to AAA.

**Step 5** The PDSN receives the MIP RRP containing a revocation support extension, and the data flow is considered to be revocable.

The following sample call flow illustrates Mobile IP Resource Revocation (HA initiated):

**Step 1** Mobile starts a mobile IP data session with PDSN/FA (1).

**Step 2** PDSN/FA (1) appends a registration revocation support extension to the mobile registration request and forwards it to the HA.

**Step 3** In response, the HA appends the registration revocation support extension to a registration reply, and send it to PDSN/FA (1).

**Step 4** PDSN-to-PDSN handoff occurs, and the Mobile re-starts a mobile IP data session with PDSN/FA (2).

**Step 5** PDSN/FA(2) sends a registration request to the HA.

**Step 6** The HA sends a registration response to PDSN/FA (2).

**Step 7** The HA sends a Mobile IP resource revocation message to the PDSN/FA (1).

**Step 8** PDSN/FA (1) sends a Mobile IP resource revocation acknowledgement to the HA, and terminates the mobile IP data session for the mobile.

The following sample call flow illustrates a Mobile IP Resource Revocation (FA initiated revocation):

**Step 1** The Mobile starts a mobile IP data session with the PDSN/FA.

**Step 2** The PDSN/FA appends the registration revocation support extension to the mobile registration request, and forwards it to the HA.

**Step 3** In response, the HA appends the registration revocation support extension to a registration reply, and sends it to the PDSN/FA.

**Step 4** Some event occurs in the PDSN/FA, and the PDSN/FA decides to close the session.

**Step 5** The PDSN/FA sends a Mobile IP resource revocation message to the HA.

**Step 6** The HA sends a Mobile IP resource revocation acknowledgement to the HA. The HA clears the binding and the PDSN/FA clears the session.

## I-bit Support

During the registration revocation phase, the I (Inform) bit notifies the mobile node (MN) of the revoked data service in cases where the mobile node has more than one MobileIP flow. If, during the registration phase, this bit is set to **1** by a mobility agent in the revocation support extension in the RRQ/RRP, it indicates that the agent supports the use of the "I" bit in revocation messages.

In the current implementation, if MobileIP RRQ is received with I bit set in the revocation support extension, then the HA also sets the I-bit to **1**, and the I-bit can be used during the revocation phase. When the HA initiates revocation (and if the I bit was negotiated), it sets the I bit to **1** in the Revocation message if a binding is administratively released, and sets it to **0** if a inter- PDSN handoff is detected by the HA. When revocation is initiated by the PDSN, and the revocation message has I-bit set to **1**, then the HA also sets the I-bit to **1** in the revocation ACK message.

## Configuring MIPv4 Registration Revocation

To enable MIPv4 Registration Revocation feature on HA, perform the following tasks in global configuration mode:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Router(config)# ip mobile home-agent revocation` | Enables support for MIPv4 Registration Revocation on the HA. |
| **Step 2** | `Router(config)# ip mobile home-agent revocation timeout` *5* `retransmit` *6* | (Optional) Sets the retransmit count and timeout value for revocation messages. |

The following example illustrates the **ip mobile home-agent revocation** command:

```
Router(config)# ip mobile home-agent revoc timeout ?
  <1-100>  Wait time (default 3 secs)
Router(config)# ip mobile home-agent revoc retransmit ?
  <0-100>  Number of retries for a transaction (default 3)
```

## Mobile IPv4 Resource Revocation Restrictions

The following list identifies the restrictions for Mobile IPv4 Resource Revocation feature for the current release:

- The STC attribute received in access-accept during HA-CHAP (MN-AAA authentication) is ignored, and the feature configuration on the Home Agent will take precedence.
- The Revocation message, Revocation ACK message, and Revocation support extension (not protected by either FHAE or IPSec) will not be discarded, but will be processed. We recommend that you configure an FA-HA security association on the Home Agent, or that an IPSec tunnel exists between the FA and the HA.

- Resource Revocation and Bind Update cannot be enabled simultaneously. Both are mutually exclusive of each other.
- The Home Agent MIB is not updated with the Registration revocation information.

### Simultaneous Bindings

The Home Agent does not support simultaneous bindings for the following reason:

- When multiple flows are established for the same NAI, a different IP address is assigned to each flow. Therefore, simultaneous binding is not required because its function is to maintain more than one flow to the same IP address.

## Radius Disconnect

Radius Disconnect (or Packet of Disconnect (PoD)) is a mechanism that allows the RADIUS server to send a Radius Disconnect Message to the HA to release resources. Resources may be released for administrative purposes, and are mainly Mobile IP bindings on the HA.

Support for Radius Disconnect on the Cisco Home Agent conforms with RFC 3576. The HA communicates its resource management capabilities to the Home AAA server in an Access Request message that is sent for authentication/authorization procedure by including a 3GPP2 Vendor Specific Session Termination Capability (STC) VSA. The value communicated in the STC VSA is obtained from configuration. The HA includes a NAS-Identifier attribute that contains its Fully Qualified Domain Name (FQDN) in the Access Request when the **radius-server attribute 32 include-in-access-req format** command is configured.

The following events occur when a Disconnect Request is received on the HA:

**Step 1** Find the user session corresponding to the username (NAI).

**Step 2** If the Framed-IP-Address attribute is received in the Disconnect Request, terminate the binding with corresponding to the address.

**Step 3** If Framed-IP-Address is not received in the Disconnect Request, terminate all bindings for the user (NAI).

### Configuring RADIUS Disconnect Client

Perform the following tasks to configure RADIUS disconnect for clients and the associated keys:

| Command | Purpose |
|---|---|
| `Router(config)# aaa pod server [clients ipaddr1 [ipaddr2] [ipaddr3] [ipaddr4]] [port port number] [auth-type {any \| all \| session-key}] [ignore session-key] {ignore server-key \| server-key string}` | Required to enable Packet of Disconnect (POD) services at AAA subsystem level in Cisco IOS. Enables inbound user sessions to be disconnected when specific session attributes are presented. |
| `Router(config)#ip mobile radius disconnect` | Enables the functionality of processing RADIUS disconnect messages on the HA. |

| Command | Purpose |
|---|---|
| `Router(config)#radius-server attribute 32 include-in-access-req` | This command is required to include the optional NAS-Identifier attribute in Access-Request to the home AAA. |
| `Router# debug aaa pod` | Displays debug information for Radius Disconnect message processing at AAA subsystem level. |

## Restrictions for RADIUS Disconnect

The following list includes restrictions for the RADIUS Disconnect feature:

- MIB is not updated with Radius Disconnect information.
- Mobile IP conditional debugging is not supported.

# Support for Binding Synch and Deletion

In the current implementation of Home Agent redundancy, bindings that are deleted on the active HA in active-standby mode (or on any peer in a peer to peer mode), due to receipt of a revocation message or a RADIUS disconnect message, are not synched to the standby HA or the peer HA. Also, the additional extensions and attributes for Revocation and Radius Disconnect are not relayed to the standby. Registration Revocation and Radius Disconnect (using the **clear ip mobile binding** command) are supported with HA redundancy. The following list identifies the benefits of this support:

#### Active-Standby Mode of HA Redundancy:

- Bindings on the active HA that are deleted by trigger (for example, receipt of a Revocation message, or a Radius Disconnect message) will be synched to the Standby HA.
- Bindings that are deleted due to commands that unconfigure (for example, **ip mobile host**, etc.), will not be synched.
- Bindings that are deleted on the standby HA will not be synched to the active in case of active-standby mode.
- Additional extensions (Revocation Support Extension) and attributes (STC attribute) for Revocation and Radius Disconnect will be relayed to the standby HA.

#### Peer-to-Peer Mode of HA Redundancy:

- Bindings that are deleted on any of the peers by trigger (for instance, a receipt of Revocation message or a Radius Disconnect message), will be synched to the other peer.
- Bindings that are deleted due to commands that unconfigure (for example, **ip mobile host**, etc.) will not be synched.
- Additional extensions (Revocation Support Extension) and attributes (STC attribute) for Revocation and Radius Disconnect will be relayed to the peer HA.

## Binding Synch

The following call flow shows the sequences and message exchange among various network entities used to bring up the Mobile IP flow and synch the information to the standby Home Agent.

1. The MS originates a call and a PPP session is up.
2. The PDSN receives a MIP RRQ from the MN and authenticates the MN by FA-CHAP. The STC VSA with the appropriate value (2 or 3) is included in the Access-request message to the AAA. After successful authentication, the PDSN forwards the RRQ to the HA and includes the revocation support extension after the MHAE.
3. The HA, upon receiving the MIP RRQ containing a revocation extension, includes a revocation support extension in the MIP RRP sent back to PDSN. During HA-CHAP to authenticate the MS, the STC VSA with appropriate value (2 or 3) is included in the Access-request message sent to the AAA. The binding at the HA is now considered revocable.
4. The PDSN receives the MIP RRP containing a revocation extension. The binding at the PDSN is revocable as the MIP RRP contained a revocation extension
5. Since the Home Agent is configured in redundant mode, a Bind Update message is sent to the standby with the additional information (revocation support extension and STC NVSE).
6. The standby Home Agent regenerates the binding using the information received in the Bind Update message, and sends back a Bind Update Ack message with code “accept” on successful creation of a binding on the standby.

## Binding Deletion

As part of this support, two new messages —“Bind Delete Request” and “Bind Delete Ack”—are introduced that are exchanged between the redundant HAs when a binding is deleted. The following sample call flow illustrates when a binding gets deleted on the active Home Agent due to receipt of Revocation message, and the deletion of binding is synched to the standby Home Agent.

1. The MS originates a call, a PPP session is up and a Mobile IP flow is setup on the active Home Agent with Registration revocation capability enabled and negotiated. The same is synched to the standby Home Agent.
2. When a user issues administrative clear command, the PDSN sends a Revocation message to the active Home Agent, deletes the visitor entry, and associated resources are cleared.
3. The active HA, upon receiving the MIP Revocation message, identifies the binding to be deleted. On identifying the binding, a Bind Delete Request message is sent out to the standby HA.
4. After a Bind Delete Request is sent out, the active HA cleans up the resources associated with the binding for the Revocation message that arrived, and sends back a MIP Revocation Ack message to the PDSN.
5. The standby HA, on receipt of Bind Delete Request message, identifies the binding to be deleted, and sends back a Bind Delete Ack message with code as “accept”.
6. If a Bind Delete Ack message is not received within a configured time on the active HA, then a Bind Delete Request message is retransmitted. This process is repeated for the max retransmit count.

During binding synch, the extensions (Revocation Support Extension) and attributes for Revocation and Radius Disconnect (STC attribute) are synched from active HA to the standby. In scenarios when the active HA goes down and the standby becomes active, the now active HA is capable of deleting bindings on receipt of a RADIUS Disconnect message. For revocation, the bindings on the now active HA are revocable, and the HA can now send and receive revocation messages.

CHAPTER 1

# Dynamic Domain Name Server Updates

This chapter discusses Domain Name Server (DNS) update methods and Server Address assignment, and provides configuration details for those features.

This chapter contains the following sections:



## IP Reachability

TIA/EIA/IS-835-D describes dynamic DNS update methods used by the home AAA server and the Home Agent. DNS update by AAA is applicable to both Simple IP and Mobile IP service, while DNS update by the Home Agent is only applicable to Mobile IP service. The following paragraphs describe the IP Reachability feature on Home Agent.

When the HA receives an initial Registration Request it sends a RADIUS Access-Request to the Home RADIUS server. If the RADIUS server is configured to request Home Agent-based DNS updates, the Home RADIUS server will include the DNS-Update-Required attribute in the RADIUS Access-Accept message returned to the HA. If the initial Mobile IP registration is successful, the HA sends a DNS Update message to the DNS server to add an A Resource Record for the MS. The HA sends a DNS Update message to the primary and secondary DNS server, if present.

When the HA receives a Mobile IP RRQ with lifetime timer set to **0**, or the Mobile IP lifetime expires, or administrative operations invalidate the mobility binding for the MS, the Home Agent will send a DNS Update message to DNS server to delete the associated Resource Record.

**Note** DNS updates are not sent for each Re-registration.

**Note** This feature is supported for Proxy Mobile IP flows as well.

The following call flow describes the IP Reachability on Home Agent - mobile registration scenario:

1. The Home Agent receives a registration request from the PDSN/FA.
2. The HA sends an access request to RADIUS Server. The HA includes DNS Server Update Capability VSA.
3. The RADIUS server sends access accept with DNS Update Required VSA.
4. The HA sends Registration response to the PDSN/FA. If the HA is configured for redundancy, the active Home Agent will sync the binding creation to the standby Home Agent.
5. The HA creates a binding, and sends DNS Update request message to DNS Server
6. The DNS Server creates a DNS entry for the NAI, and sends DNS Update response message to the HA.

The following call flow describes the IP Reachability on Home Agent - Mobile deregistration scenario:

1. The Home Agent receives a registration request with lifetime zero from PDSN/FA.
2. The HAsends an access request to RADIUS Server, if SA is not stored locally (optional).
3. The RADIUS Server sends access accept (optional).
4. The HA deletes the binding and sends a Registration response to PDSN/FA. If the HA is configured for redundancy, the active HA will sync the binding deletion to standby HA.
5. The HA sends a DNS Update request message to DNS Server to delete the DNS entry.
6. The DNS Server deletes the DNS entry for the NAI, and sends a DNS Update response message to the HA.

## Configuring IP Reachability

The following commands will enable the IP Reachability feature on Home Agent for the specified realm:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Router(config)# ip name-server x.x.x.x` | Specifies the address of one or more name servers to use for name and address resolution. |
| **Step 2** | `Router(config)# ip mobile realm @ispxyz1.com dns dynamic-update method word` | Enables the DNS Update procedure for the specified realm. *word* is the dynamic DNS update method name. |
| **Step 1** | `Router(config)# ip mobile realm realm dns server primary dns server address secondary dns server address` | Allows you to locally configure the DNS Server address. |

To verify that this feature is enabled for a binding, use the following command:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Router# show ip mobile binding` | Displays the mobility binding table. |

The following example illustrates the realm configuration for IP reachability:

```
ip ddns update method sit-ha2-ddns2
 DDNS both
ip mobile realm @ispxyz2.com dns dynamic-update method sit-ha2-ddns2
```

# DNS Server Address Assignment

IS835D defines a method to push the home DNS server address to a mobile as an NVSE in a mobileip registration response. This procedure allows the Mobile Station to learn the primary and secondary DNS server address of its home domain.

The RADIUS server includes a DNS Server VSA in an access response to the HA during mobile authentication. The HA forms a DNS server NVSE from the DNS Server VSA and adds it to mobileip registration response. If the DNS Server VSA is not received at the time of authentication, and a DNS server address is configured locally on the HA, the HA will form a DNS server NVSE from the local configuration and add it to mobileip registration response.

The DNS Server VSA and DNS Server NVSE carry primary and secondary DNS IP addresses.

The DNS Server VSA will be synced to the standby if the HA is deployed in redundant mode.

To enable this feature for the specified realm, issue the following commands:

ip mobile realm *realm* dns server assign

ip name-server x.x.x.x

To locally configure the DNS Server address, issue the following command:

**ip mobile realm** *realm* **dns server** *primary dns server address secondary dns server address*

To verify that this feature is enabled for a binding, use the **show ip mobile binding** command.

**Note** If the DNS server address is configured both locally and downloaded from AAA, then preference will be given to the local configuration on the HA.

# Examples

The following example illustrates how to configure a User profile for DNS:

```
[ //localhost/Radius/Profiles/mwts-mip-r20sit-haslb1-prof/Attributes ]
    CDMA-DNS-Server-IP-Address = 01:06:0A:4D:9B:0A:02:06:0A:4D:9B:09:03:03:01:04:03:01
    CDMA-DNS-Update-Required = "HA does need to send DNS Update"
    CDMA-HA-IP-Addr = 20.20.225.1
    CDMA-MN-HA-Shared-Key = ciscociscociscoc
    CDMA-MN-HA-SPI = 00:00:10:01
    CDMA-Reverse-Tunnel-Spec = "Reverse tunneling is required"
    class = "Entering the World of Mobile IP-3"
    Service-Type = Framed
```

Here is a sample configuration of the DNS server address assignment realm:

```
ip mobile realm @ispxyz2.com dns server 10.77.155.10 2.2.2.2
ip mobile realm @ispxyz2.com dns server assign
```

The following example illustrates how to configure the same in an AR user profile:

```
set  CDMA-DNS-Server-IP-Address 01:06:0A:4D:9B:0A:02:06:0A:4D:9B:09:03:03:01:04:03:01
```

**Bold** text are the primary and secondary DNS server addresses.

Here is a sample configuration of both IP Reachability and DNS Server Address Assignment:

```
ha2#show run
Building configuration...

Current configuration : 10649 bytes
!
! Last configuration change at 22:45:21 UTC Fri Nov 11 2005
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
service udp-small-servers
!
hostname tb1-6513-ha2
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa group server radius MOT
 server 150.2.0.1 auth-port 1645 acct-port 1646
!
aaa authentication ppp default local group MOT
aaa authorization config-commands
aaa authorization ipmobile default group MOT
aaa authorization network default group MOT
aaa authorization configuration default group MOT
aaa accounting session-duration ntp-adjusted
aaa accounting update newinfo periodic 3
aaa accounting network ha start-stop group MOT
aaa accounting system default start-stop group MOT
!
aaa server radius dynamic-author
 client 150.2.0.1
 server-key cisco
!
aaa session-id common
!
resource policy
!
ip subnet-zero
no ip gratuitous-arps
!
!
ip cef
ip dfp agent ipmobile
 port 400
 interval 15
 inservice
!
ip ftp source-interface GigabitEthernet0/0.10
ip ftp username root
ip ftp password pdsnmwg
```

```
no ip domain lookup
ip name-server 10.77.155.10
ip name-server 1.1.1.1
ip name-server 6.6.6.6
no ip dhcp use vrf connected
no ip dhcp conflict logging
ip dhcp ping packets 0
!
ip dhcp pool Subnet-Pool1
   utilization mark high 75
   utilization mark low 25
   origin dhcp subnet size initial /30 autogrow /30
!
!
ip vrf forwarding
!
ip vrf ispxyz
!
ip vrf ispxyz-vrf1
 rd 100:1
!
ip vrf ispxyz-vrf2
 rd 100:2
!
!
ip ddns update method sit-ha2-ddns1
 DDNS both
!
ip ddns update method sit-ha2-ddns2
 DDNS both
!
vpdn enable
vpdn ip udp ignore checksum
!
vpdn-group testsip1-l2tp
! Default L2TP VPDN group
! Default PPTP VPDN group
 accept-dialin
  protocol any
  virtual-template 1
 l2tp tunnel hello 0
!
username user-ha2 password 0 cisco
!
!
!
interface Tunnel10
 no ip address
 ip access-group 150 in
!
interface Loopback0
 ip address 20.20.225.1 255.255.255.0
!
interface Loopback1
 description address of the LNS server
 ip address 20.20.206.20 255.255.255.0
!
interface Loopback2
 ip address 170.12.0.102 255.255.0.0
!
interface GigabitEthernet0/0
 no ip address
 no ip route-cache cef
 no ip route-cache
```

```
 no keepalive
 no cdp enable
!
interface GigabitEthernet0/0.10
 description TFTP vlan
 encapsulation dot1Q 10
 ip address 10.77.155.5 255.255.255.192
 no ip route-cache
 no snmp trap link-status
 no cdp enable
!
interface GigabitEthernet0/0.172
 description HAAA interface
 encapsulation dot1Q 172
 ip address 170.2.0.20 255.255.0.0
 no ip route-cache
 no snmp trap link-status
 no cdp enable
 standby delay minimum 15 reload 15
 standby version 2
 standby 2 ip 170.2.0.102
 standby 2 follow sit-ha2
!
interface GigabitEthernet0/0.202
 description PI interface
 encapsulation dot1Q 202
 ip address 20.20.202.20 255.255.255.0
 no ip route-cache
 no snmp trap link-status
 no cdp enable
 standby delay minimum 15 reload 15
 standby version 2
 standby 2 ip 20.20.202.102
 standby 2 ip 20.20.204.2 secondary
 standby 2 ip 20.20.204.3 secondary
 standby 2 ip 20.20.204.4 secondary
 standby 2 ip 20.20.204.5 secondary
 standby 2 ip 20.20.204.6 secondary
 standby 2 timers msec 750 msec 2250
 standby 2 priority 130
 standby 2 preempt delay minimum 180
 standby 2 name sit-ha2
!
interface GigabitEthernet0/0.205
 description REF interface
 encapsulation dot1Q 205
 ip address 20.20.205.20 255.255.255.0
 no ip route-cache
 no snmp trap link-status
 no cdp enable
 standby delay minimum 15 reload 15
 standby version 2
 standby 2 ip 20.20.205.102
 standby 2 follow sit-ha2
!
interface Virtual-Template1
 description To be used by VPDN for PPP tunnel
 ip unnumbered Loopback1
 peer default ip address pool LNS-pool
 no keepalive
 ppp accm 0
 ppp authentication chap pap optional
 ppp accounting none
!
```

```
router mobile
!
ip local pool LNS-pool 7.0.0.1 7.0.0.255
ip local pool ispxyz-vrf1-pool 50.0.0.1 50.0.0.255
ip local pool mobilenodes 40.0.0.1 40.0.100.255
ip default-gateway 10.77.155.1
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0.202
ip route 10.77.139.29 255.255.255.255 10.77.155.1
ip route 150.2.0.0 255.255.0.0 170.2.0.1
no ip http server
!
!
ip mobile debug include username
ip mobile home-agent template Tunnel10 address 20.20.202.102
ip mobile home-agent revocation timeout 5 retransmit 4
ip mobile home-agent dynamic-address 20.20.202.102
ip mobile home-agent accounting ha broadcast lifetime 3600 replay 8 suppress-unreachable
unknown-ha deny
ip mobile home-agent redundancy sit-ha2 virtual-network address 20.20.202.102
periodic-sync
ip mobile radius disconnect
ip mobile virtual-network 50.0.0.0 255.0.0.0
ip mobile virtual-network 40.0.0.0 255.0.0.0
ip mobile host nai mwts-pmp-r20sit-base-user1@ispxyz1.com virtual-network 40.0.0.0
255.0.0.0 aaa load-sa lifetime 600
ip mobile host nai @ispxyz2.com address pool local mobilenodes virtual-network 40.0.0.0
255.0.0.0 aaa lifetime 180
ip mobile realm mwts-pmp-r20sit-base-user1@ispxyz1.com dns server 10.77.155.10 1.1.1.1
ip mobile realm mwts-pmp-r20sit-base-user1@ispxyz1.com dns server assign
ip mobile realm mwts-pmp-r20sit-base-user1@ispxyz1.com dns dynamic-update method
sit-ha2-ddns1
ip mobile realm @ispxyz2.com vrf ispxyz-vrf2 ha-addr 20.20.204.6
ip mobile realm @ispxyz2.com dns server 10.77.155.10 2.2.2.2
ip mobile realm @ispxyz2.com dns server assign
ip mobile realm @ispxyz2.com dns dynamic-update method sit-ha2-ddns2
ip mobile secure foreign-agent 20.20.201.10 20.20.201.100 spi 100 key ascii cisco replay
timestamp within 7 algorithm md5 mode prefix-suffix
ip mobile secure foreign-agent 20.20.210.10 20.20.210.100 spi 100 key ascii cisco replay
timestamp within 5 algorithm md5 mode prefix-suffix
ip mobile secure home-agent 20.20.202.10 20.20.202.95 spi 100 key ascii cisco replay
timestamp within 7 algorithm md5 mode prefix-suffix
!
ip radius source-interface Loopback2
no logging trap
logging source-interface GigabitEthernet0/0.201
access-list 150 permit ip host 40.0.0.1 host 20.20.205.220 log
access-list 150 permit ip host 20.20.205.220 host 40.0.0.1 log
access-list 150 deny   ip any any log
snmp-server community public RO
snmp-server community private RW
snmp-server trap-source Loopback0
snmp-server host 150.2.0.100 version 2c private
snmp-server host 150.2.0.100 public
no cdp run
!
!
radius-server attribute 44 include-in-access-req
radius-server attribute 8 include-in-access-req
radius-server attribute 32 include-in-access-req
radius-server attribute 55 access-request include
radius-server host 150.2.0.1 auth-port 1645 acct-port 1646 key 7 121A0C041104
radius-server host 150.2.0.100 auth-port 1645 acct-port 1646 key cisco
radius-server retransmit 4
```

```
radius-server timeout 2
radius-server deadtime 5
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
radius-server vsa send accounting 3gpp2
radius-server vsa send authentication 3gpp2
!
control-plane
!
alias exec shc sh cdma pdsn
alias exec ua undebug all
alias exec ui undebug ip packet
!
line con 0
 exec-timeout 0 0
line vty 0 4
 exec-timeout 0 0
line vty 5 15
 exec-timeout 0 0
!
!
end
```

ha2#

CHAPTER 1

# Per User Packet Filtering

This chapter discusses Per-User Packet Filtering and its implementation in Cisco IOS Mobile Wireless Home Agent software.

This chapter includes the following sections:



## Mobile-User ACLs in Packet Filtering

The Home Agent supports per user packet filtering. Packet filtering provides that, for a successfully authenticated registration request, the RADIUS server will return “inACL” and “outACL” attributes in an access response to the HA. “inACL” and “outACL” attributes identify the pre-configured ACLs on the HA that are applied to mobility bindings. An input ACL applies to traffic from the user leaving the tunnel. An output ACL applies to traffic sent to the user using the tunnel. The attributes are synched to the standby HA during normal sync and bulksync operation. Here are some additional conditions associate with this feature:

- The **show ip mobile binding** command displays ACLs applied to a mobility binding. Only the ACLs downloaded at the time of initial authentication are applied. An ACL downloaded at the time of mobile re-authentication, for lifetime renewal, is not applied.
- The HA will accept one input ACL name and one output ACL name for each user.
- Only named extended access-lists are supported for this feature.

**Note** Performance is significantly degraded when mobile user ACLs are applied to a large number of mobility bindings.

The Home Agent can filter both egress packets from an external data network and ingress data packets based on the Foreign Agent IP address or the Mobile Node IP address.

## Configuring ACLs on the Tunnel Interface

To configure ACLs to block certain traffic using the template tunnel feature, perform the following task:

| Command | Purpose |
|---|---|
| `Router(config)# interface tunnel 10`<br>`ip access-group 150 in -------> apply access-list 150`<br>`access-list 150 deny any 10.10.0.0 0.255.255.255`<br>`access-list permit any any`<br>`------> permit all but traffic to 10.10.0.0 network`<br><br>`ip mobile home-agent template tunnel 10 address 10.0.0.1` | Configures a tunnel template.<br>Configures the ACL.<br><br>Configures a Home Agent to use the template tunnel. |

## Verifying ACLs are Applied to a Tunnel

Here is example output of the **show ip mobile binding** command:

### ACLs Applied to a Mobility Binding and Accounting Session ID and Accounting Counters

```
router# show ip mobile binding 44.0.0.1
Mobility Binding List:
    44.0.0.1:
    Care-of Addr 55.0.0.11, Src Addr 55.0.0.11
    Lifetime granted 00:01:30 (90), remaining 00:00:51
    Flags sbDmg-T-, Identification C661D5A0.4188908
    Tunnel1 src 46.0.0.3 dest 55.0.0.11 reverse-allowed
    Tunnel1 Input ACL: inaclname
    Tunnel1 Output ACL: outaclname - Empty list or not configured.
    MR Tunnel1 src 46.0.0.3 dest 55.0.0.11 reverse-allowed
    Routing Options - (D)Direct-to-MN (T)Reverse-tunnel
    Mobile Networks: 111.0.0.0/255.0.0.0 (S)
    Acct-Session-Id: 0
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes

router# show ip mobile tunnel

Mobile Tunnels:
    Total mobile ip tunnels 1
    Tunnel0:
    src 46.0.0.3, dest 55.0.0.11
    encap IP/IP, mode reverse-allowed, tunnel-users 1
    Input ACL users 1, Output ACL users 1
    IP MTU 1480 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Ethernet1/0
    HA created, fast switching enabled, ICMP unreachable enabled
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 drops
0 packets output, 0 bytes
```

CHAPTER 1

# Home Agent Security

# Security

This chapter discusses the concepts that comprise the Security features in Cisco IOS Mobile Wireless Home Agent software.

This chapter includes the following sections:



## 3 DES Encryption

The Cisco Home Agent includes 3DES encryption, which supports IPSec on the HA. To accomplish this on the Cisco 7200 Internet router platform, Cisco supplies an SA-ISA card for hardware provided IPsec. On the Cisco 7600 and Cisco 6500 Catalyst switch platforms, the MWAM utilizes the Cisco IPSec Acceleration Card.

The HA requires you to configure the parameters for each PDSN before a mobile IP data traffic tunnel is established between the PDSN and the HA.

**Note** This feature is only available with hardware support.

# Mobile IP IPSec

The Internet Engineering Task Force (IETF) has developed a framework of open standards called IP Security (IPSec) that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer; it uses Internet Key Exchange (IKE) to handle negotiation of protocols and algorithms based on local policy, and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

The HA uses any statically configured shared secret(s) when processing authentication extension(s) present in mobile IP registration messages.

The HA supports IPSec, IKE, Authentication Header (AH) and IP Encapsulating Security Payload (ESP) as required in IS-835-B.

IS835-B specifies three mechanisms for providing IPSec security:

- Certificates
- Dynamically distributed pre-shared secret
- Statically configured pre-shared secret.

**Note** IS835B Static IPSec feature is available only on the Cisco 7200 Internet router platform. The Cisco IOS IPSec feature is available on the Cisco 7200 Internet router, Cisco 6500 Catalyst switch, and Cisco 7600 switch platforms. The HA 2.0 (and above) Release only supports statically configured, pre-shared secret for IPSec IKE.

As per IS-835-B, The HA and AAA should be configured with same security level for a PDSN. The PDSN receives a security level from AAA server and initiates IKE, and the HA responds to the IKE request for establishing security policy.

The PDSN receives a security level from the AAA server and initiates IKE, and the HA responds to the IKE request for establishing a security policy. All traffic specified by the access-list of the crypto configuration is protected by the IPSec tunnel. The access-list is configured to protect all traffic between the PDSN and HA, and all bindings belonging to a given PDSN-HA pair are protected.

IPSec is not applicable to mobiles using Co-located COA

**Note** Cisco Mobile Wirelesss Home Agent Release 2.0 (and above) on the Cisco 7600 and Cisco 6500 Catalyst platforms requires the support of the Cisco IPSec Services Module (VPNSM), a blade that runs on the Catalyst 6500 or 7600 router. VPNSM does not have any physical WAN or LAN interfaces, and utilizes VLAN selectors for its VPN policy.

For more information on Catalyst 6500 Security Modules visit http://www.cisco.com/en/US/products/hw/switches/ps708/index.html.

For more information on the Cisco 7600 Internet Router visit http://www.cisco.com/en/US/products/hw/routers/ps368/index.html.

IPSec-based security may be applied on tunnels between the PDSN and the HA depending on parameters received from the Home AAA server. A single tunnel may be established between each PDSN-HA pair. It is possible for a single tunnel between the PDSN-HA pair to have three types of traffic streams: Control Messages, Data with IP-in-IP encapsulation, and Data with GRE-in-IP encapsulation. All traffic carried in the tunnel has the same level of protection provided by IPSec.

IS835 defines MobileIP service as described in RFC 2002; the Cisco Mobile Wireless HA provides Mobile IP service and Proxy Mobile IP service.

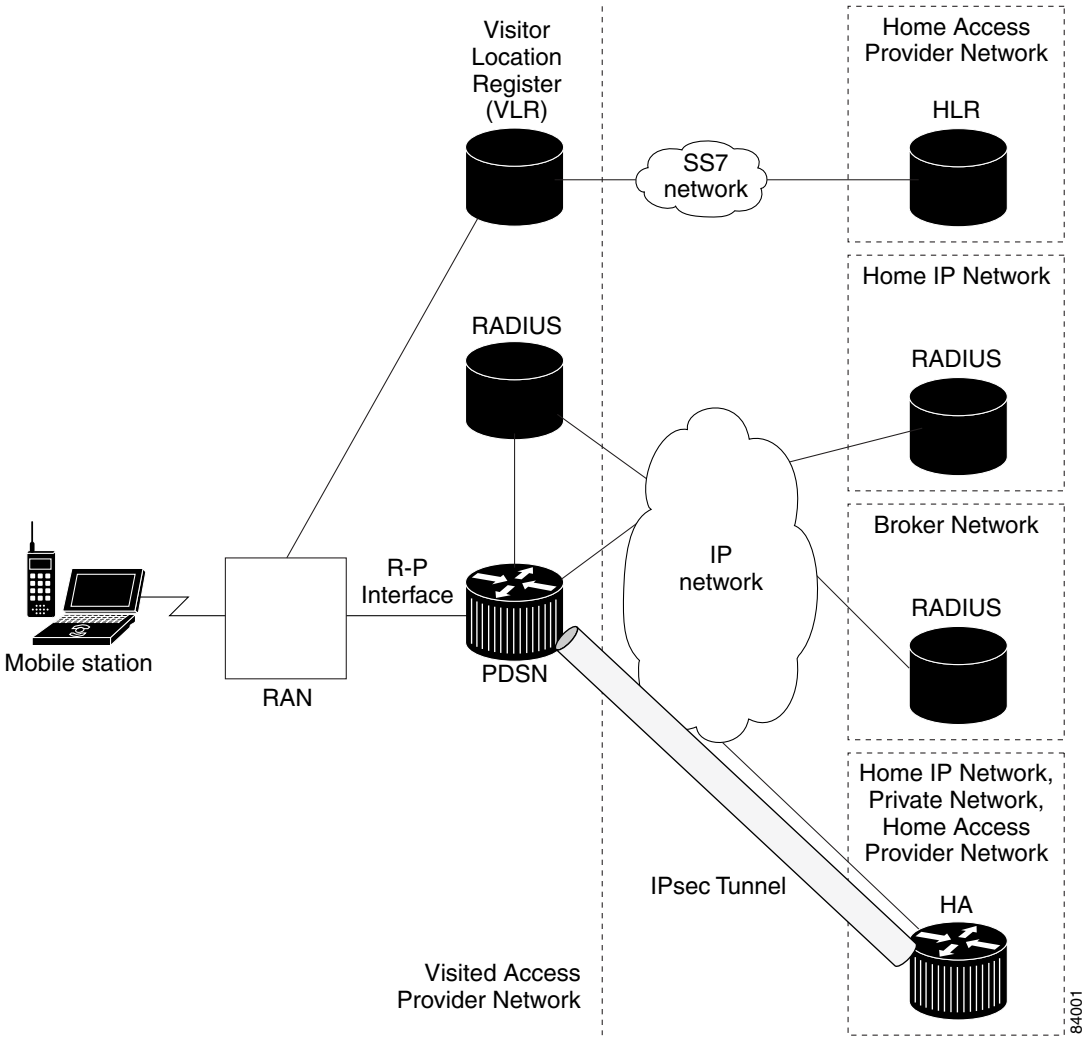
In Proxy Mobile service, the Mobile-Node is connected to the PDSN/FA through Simple IP, and the PDSN/FA acts as Mobile IP Proxy for the MN to the HA.

Once Security Associations (SAs or tunnels) are established, they remain active until there is traffic on the tunnel, or the lifetime of the SAs expire.

**Note** IPSec does not work with HA redundancy, since the IPSec security associations are not replicated to the standby during failover.

Figure 1-1 illustrates the IS835 IPSec network topology.

***Figure 1-1 IS835 IPSec Network***



# IPSec Interoperability Between the PDSN and HA (IS-835-C)

IPSec rules under IS-835C mandates that connections are always initiated from the PDSN to the Home Agent IP address. Certain PDSNs may not be flexible in their approach to IPSec configuration. These PDSNs do not allow any configuration for Remote IPSec termination points, and expect that the remote IPSec termination point is always the Home Agent IP address.

The following section illustrates how to handle IPSec Interoperability between such PDSNs and the HA with Home Agent.

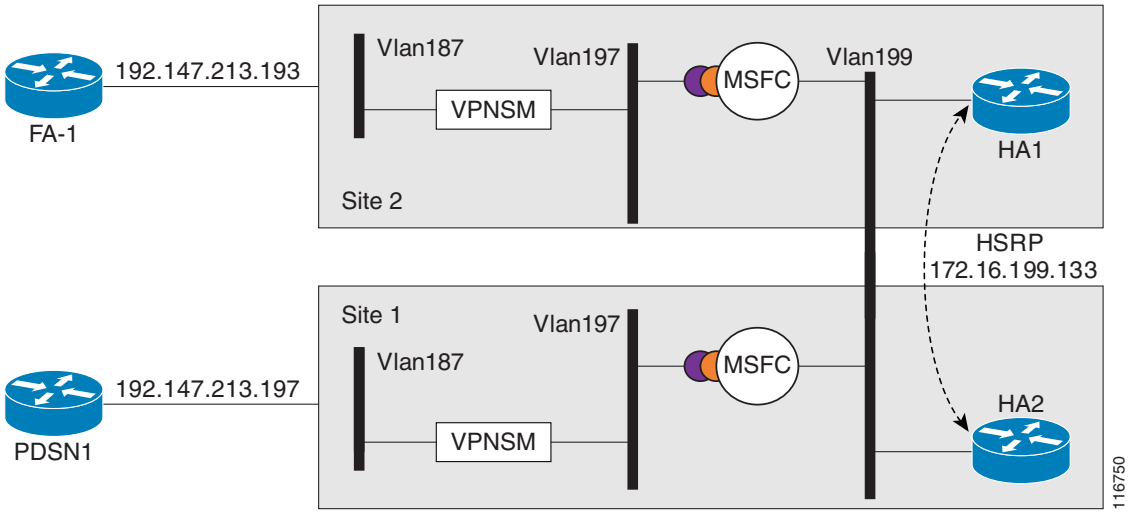
The change in the configuration allows for IPSec connections for the Home Agent IP address that are still terminated by the VPNSM.

### Handling Single Home Agent Instance

This solution is achieved by letting SUP IOS own the same Home Agent IP address. Traffic to the Home Agent is then policy routed to the correct Home Agent.

Figure 1-2 illustrates a possible configuration:

***Figure 1-2 Single HA Interoperability***




Here is a sample configuration for the Supervisor. The PDSN IP Address is 14.0.0.1, HA3 address is 13.0.0.50, and HA4 is 13.0.0.51

### Single HA Instance - Interoperability

```
crypto isakmp policy 1
 hash md5
 authentication pre-share
 lifetime 60000
crypto isakmp key cisco address 10.0.0.0 0.0.0.0
!
crypto ipsec transform-set mobile-set1 esp-3des

# Comment: testmap is used for HA3

crypto map testmap local-address Loopback21
crypto map testmap 20 ipsec-isakmp
 set peer 10.0.0.1
```

```
 set transform-set mobile-set1
 match address 131
!

interface Loopback21
 description corresponds to ha-on-proc3
 ip address 10.0.0.50 255.255.255.255
!

interface GigabitEthernet4/1
description encrypt traffic from vlan 151 to vlan 201& 136 to 139
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,136,146,151,1002-1005
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet4/2
 description decrypts traffic from vlan 201 to 151, 139 to 136
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,139,149,201,1002-1005
 switchport mode trunk
 cdp enable

interface Vlan136
 description secure vlan
 ip address 10.0.0.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA3
 no mop enabled
 crypto map testmap
!
interface Vlan137
 description internal vlan to HA3
 ip address 10.0.0.1 255.255.0.0
!
interface Vlan139
 no ip address
 crypto connect vlan 136
!

access-list 131 permit ip host 10.0.0.1 host 10.0.0.50
access-list 131 permit ip host 10.0.0.50 host 10.0.0.1
access-list 131 permit ip 10.0.0.0 0.0.0.255 10.0.0.0 0.0.0.255

access-list 2000 permit udp any any eq mobile-ip
access-list 2000 permit ipinip any any

route-map RRQ-HA3 permit 10
 match ip address 2000
 set ip next-hop 10.0.0.2
!
```

# IPSec Support on Catalyst 6500/7600 with 5 CPUs of MWAM

You may require an IPSec tunnel be established over the mobile IP tunnel between the PDSN and the HA. The PDSN resides in the foreign network and the HA in the home network. As per IS-835B specification, IPSec connections are always initiated from the PDSN towards the HA, so the IPSec tunnel endpoints are the PDSN IP address and the HA IP address.

In Cisco's 6500 Catalyst and 7600 HA solution, IPSec is terminated at the Supervisor (SUP), while the actual HA application resides on the MWAM card(s). Each MWAM card has 5 CPUs, each running one HA instance. Each HA has its own IP address. If different IP addresses are used in the SUP as IPSec endpoints, and in the MWAM for HA endpoints, IKE messages generated from the PDSN with HA IP addresses are dropped at the SUP.

To avoid this issue, the above requirement is achieved by letting the SUP own the same IP address that is configured as the HA IP address on the MWAM. The requirement is to split the IPSec traffic for different HA IP addresses across separate IPSec VLANs so that each PDSN-HA pair is handled appropriately. This configuration allows the SUP to support all 5 CPUs on the MWAM card running the HA application, each owning an IP address that is the IPSec endpoint.

In this case, the VRF IPSec feature on the SUP720 is used. All traffic coming from the PDSN is put on different VLANs based on the HA IP address. Each VLAN corresponds to one VRF and one VRF exists per HA instance on the SUP. In this situation, the VRF mode of IPSec is used to split traffic between the 5 different HA instances present on the MWAM. Once the packets are decrypted by the crypto VLAN, packets are then policy routed using an internal VLAN that corresponds to the particular HA to the correct HA CPU on the MWAM.

IPSec redundancy across chassis and within a single chassis is supported for this environment.

The following call flow describes this behavior:

1. An IPSec security association (SA) is opened between each PDSN and HA IP address pair on the SUP. IKE messages are sent from the PDSN with its IP address and peer IP address as the particular HA IP address. Based on the PDSN IP address and the HA IP address in the IKE message, the correct ISAKMP profile is selected for the PDSN-HA pair that indicates the VRF for the pair. This establishes different SPIs corresponding to the PDSN-HA pair.
2. One VLAN per HA IP address is defined, and it belongs to a VRF that is defined for that IP address on the SUP. Thus, the SUP owns the HA IP address, and it is the IPSec terminating point for PDSN.
3. Once an IPSec SA is established between each PDSN-HA IP address pair, encrypted packets are put on to the correct VRF based on the SPI of the incoming packet.
4. Once the encrypted packets are decrypted at the IPSec VLAN corresponding to the HA address, the packets are policy routed to the corresponding CPU on the MWAM card that hosts the HA IP address (using the internal VLAN present between SUP and the HA instance on the MWAM).
5. In the return path, packets from HA instances on the MWAM are placed on the internal VLAN and put on to the corresponding IPSec VLAN for the HA. This enables the packet to be encrypted and sent out to the PDSN using the outgoing interface.

# Restrictions

### Simultaneous Bindings

The Cisco Home Agent does not support simultaneous bindings. When multiple flows are established for the same NAI, a different IP address is assigned to each flow. This means that simultaneous binding is not required, because it is used to maintain more than one flow to the same IP address.

### Security

The HA supports IPSec, IKE, IPSec Authentication Header (AH) and IP Encapsulating Security Payload (ESP) as required in IS-835-B. The Home Agent does not support security for control or user traffic independently. Either both are secured, or neither.

The Home Agent does not support dynamically assigned keys or shared secrets as defined in IS-835-B.

## Configuring Mobile IP Security Associations

To configure security associations for mobile hosts, FAs, and HAs, use one of the following commands in global configuration mode:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Router(config)# ip mobile secure {host \| visitor \| home-agent \| foreign-agent \| proxy-host} {lower-address [upper-address] \| nai string} {inbound-spi spi-in outbound-spi spi-out \| spi spi} key {hex \| ascii} string [replay timestamp [number] algorithm md5 mode prefix-suffix]` | Specifies the security associations for IP mobile users. |

## Configuring IPSec for the HA

To configure IPSec for the HA, use the following commands in global configuration mode:

| | Command | Purpose |
|---|---|---|
| **Step 1** | Router(config)# **crypto map** *map-name seq-num* **ipsec-isakmp**<br><br>**set peer** *ip address of ha*<br>**set transform-set** transform-set-name<br>**match address** *acl name*<br><br>**crypto map** *map name* **local-address** *interface* | Creates a a crypto map entry for one HA in one Crypto-map set.<br>The Crypto Map definition is not complete until:<br>1. ACL associated with it is defined, and<br>2. The Crypto-Map is applied on the interface. You can configure Crypto MAP for different HAs by using a different sequence number for each HA in one crypto-map set.<br><br>Specifies and names an identifying interface to be used by the crypto map for IPSec traffic. |
| **Step 2** | Router# **access-list** *acl-name* **deny udp host** *HA IP addr* **eq mobile-ip host** *PDSN IP addr* **eq mobile-ip**<br><br>**access-list** *acl-name* **permit ip host** *PDSN IP addr* **host** *HA IP addr*<br><br>**access-list** *acl-name* **deny ip any any** | Defines the access list.<br>The ACL name “acl-name” is same as in the crypto-map configuration. |
| **Step 3** | Router# **Interface** *Physical-Interface of PI interface*<br><br>**crypto map** *Crypto-Map set* | Applies the Crypto-Map on Pi Interface, as the HA sends/receives Mobile IP traffic to/from PDSN on this interface. |

## Creating Active Standby Home Agent Security Associations

The following IOS command displays active standby Home Agent security associations:

| | Command | Purpose |
|---|---|---|
| **Step 1** | Router(config)#**show ip mobile secure ?**<br><br>**foreign-agent**<br>**home-agent**<br>**host**<br>**summary** | Displays the active and standby Home Agent Security associations.<br>Displays Foreign agent security associations. Displays Home agent security associations. Displays Mobile host security associations. Displays a summary of security associations. |

Here is an example of the command:

```
Router# show ip mobile secure home-agent
Security Associations (algorithm,mode,replay protection,key):
30.0.0.30:
   SPI 100,  MD5, Prefix-suffix, Timestamp +/- 7,
   Key 'red'
HA#
```

# Configuration Examples

## Home Agent IPSec Configuration

**Note** Once you permit the hosts/subnets you want encrypted, ensure that you put in an explicit deny statement. The deny statement states do not encrypt any other packets.

**Note** The following example is for IPSec on the Cisco 7200 router only. IPSec on the Cisco Catalyst 6500 amd the 7600 is configured on the Supervisor, rather than on the Home Agent.

```
access-list 101 deny   ip any any
access-list 103 deny   ip any any

------------------------------------------------------

!
! No configuration change since last restart
!
version 12.2
service timestamps debug datetime
service timestamps log datetime
service password-encryption
!
hostname 7206f1
!
aaa new-model
!
!
aaa authentication login CONSOLE none
aaa authentication login NO_AUTHENT none
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa session-id common
enable password 7 151E0A0E
!
username xxx privilege 15 nopassword
ip subnet-zero
ip cef
!
!
no ip domain-lookup
!
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 10.1.1.4
crypto isakmp key cisco address 172.16.60.30
!
!
crypto ipsec transform-set esp-des-sha-transport esp-des esp-sha-hmac
 mode transport
!
crypto map tosim 10 ipsec-isakmp
```

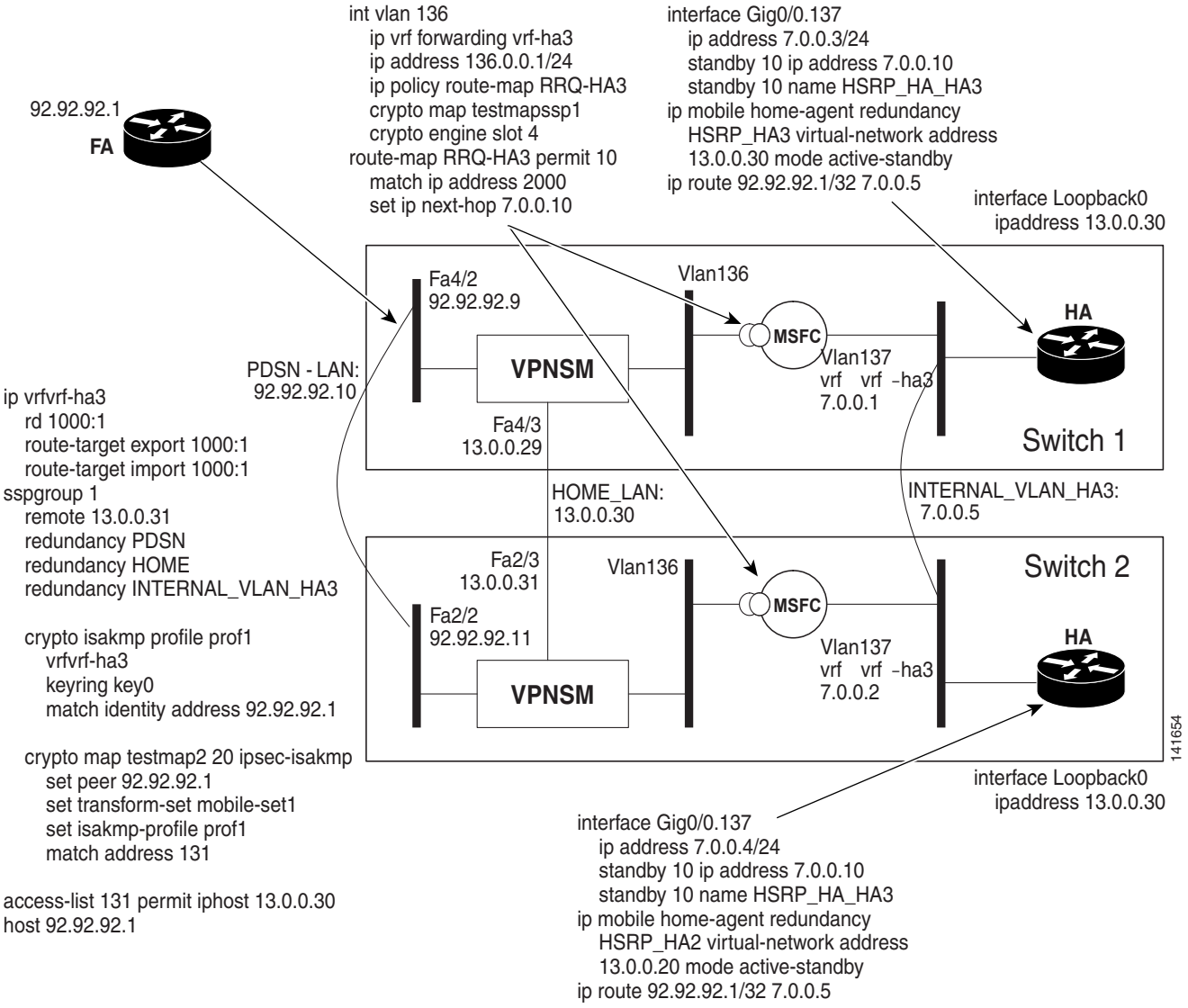
```
 set peer 10.1.1.4
 set transform-set esp-des-sha-transport
 match address 101
!
crypto map tosim3 10 ipsec-isakmp
 set peer 172.16.60.30
 set transform-set esp-des-sha-transport
 match address 103
!
!
interface Loopback0
 ip address 10.0.0.1 255.0.0.0
!
interface Loopback1
 ip address 10.0.0.9 255.0.0.0
!
interface Loopback10
 ip address 10.1.1.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 10.1.1.9 255.255.255.0
 load-interval 30
 duplex full
 speed 100
 crypto map tosim
!
interface FastEthernet0/1
 ip address 10.1.1.1 255.0.0.0
 load-interval 30
 duplex full
 speed 100
!
interface FastEthernet1/0
 ip address 10.1.1.9 255.255.255.0
 load-interval 30
 duplex full
!
interface FastEthernet2/0
 ip address 172.16.60.10 255.255.255.0
 load-interval 30
 duplex full
 crypto map tosim3
!
router mobile
!
ip local pool ispabc-pool1 10.0.0.2 12.1.0.1
ip local pool ispabc-pool1 10.1.0.8 12.2.0.1
ip local pool ispxyz-pool1 10.0.0.2 9.1.0.1
ip local pool ispxyz-pool1 10.1.0.8 9.2.0.1
ip classless
ip route 172.16.49.48 255.255.255.255 172.16.60.1
no ip http server
ip pim bidir-enable
ip mobile home-agent address 10.1.1.1
ip mobile host nai @ispabc.com address pool local ispabc-pool1 virtual-network 10.0.0.0
255.0.0.0 aaa load-sa lifetime 65535
ip mobile host nai @ispxyz.com address pool local ispxyz-pool1 virtual-network 10.0.0.9
255.0.0.0 aaa load-sa lifetime 65535
!
!
access-list 101 permit ip host 10.1.1.1 host 1.1.1.4
access-list 101 deny   ip any any
access-list 103 permit ip host 10.1.1.1 host 172.16.60.30
access-list 103 deny   ip any any
```

```
!
!
radius-server host 172.16.49.48 auth-port 1645 acct-port 1646 key 7 094F471A1A0A
radius-server retransmit 3
radius-server key 7 02050D480809
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 exec-timeout 0 0
!
exception protocol ftp
exception dump 64.102.16.25
exception memory minimum 1000000
ntp clock-period 17179878
ntp server 172.16.60.1
!
end
```

## Configuration - SUP720 / VRF-IPSec for 5 HA Instances

The following example provides detail of the SUP720 / VRF-IPSec configuration, as illustrated in Figure 1-3.

***Figure 1-3 SUP720 / VRF-IPSec Configuration***



## SUP Configuration - Switch 1:

```
ip vrf vrf-ha2
 rd 2000:1
 route-target export 2000:1
 route-target import 2000:1
!
ip vrf vrf-ha3
 rd 1000:1
 route-target export 1000:1
 route-target import 1000:1
!
ip vrf vrf-ha4
 rd 4000:1
 route-target export 4000:1
 route-target import 4000:1
!
ip vrf vrf-ha5
 rd 5000:1
 route-target export 5000:1
 route-target import 5000:1
!
ip vrf vrf-ha6
 rd 6000:1
 route-target export 6000:1
 route-target import 6000:1
!
ssp group 1
 remote 13.0.0.31
 redundancy PDSN-LAN
 redundancy HOME-LAN
 redundancy INTERNAL_VLAN_HA3
 redundancy HOME-LAN-2
 redundancy INTERNAL_VLAN_HA2
 redundancy HOME-LAN-4
 redundancy HOME-LAN-5
 redundancy HOME-LAN-6
 redundancy INTERNAL_VLAN_HA4
 redundancy INTERNAL_VLAN_HA5
 redundancy INTERNAL_VLAN_HA6
 port 4098
!
crypto keyring key0
  pre-shared-key address 92.92.92.1 key cisco
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 60000
crypto isakmp ssp 1
!
crypto isakmp profile prof1
   vrf vrf-ha2
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 12.0.0.30
crypto isakmp profile prof2
   vrf vrf-ha3
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 13.0.0.30
crypto isakmp profile prof4
   vrf vrf-ha4
```

```
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 14.0.0.30
crypto isakmp profile prof5
   vrf vrf-ha5
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 15.0.0.30
crypto isakmp profile prof6
   vrf vrf-ha6
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 16.0.0.30
!
crypto ipsec transform-set mobile-set1 esp-des esp-sha-hmac
!
crypto map testmap local-address FastEthernet4/3
crypto map testmap 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof2
 match address 131
!
crypto map testmap1 local-address FastEthernet4/4
crypto map testmap1 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof1
 match address 121
!
crypto map testmap4 local-address FastEthernet4/7
crypto map testmap4 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof4
 match address 141
!
crypto map testmap5 local-address FastEthernet4/9
crypto map testmap5 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof5
 match address 151
!
crypto map testmap6 local-address FastEthernet4/11
crypto map testmap6 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof6
 match address 161
!
crypto engine mode vrf
!
interface FastEthernet4/2
 ip address 92.92.92.9 255.255.0.0
 ip policy route-map RRQ-HA10
 speed 100
 duplex half
 standby delay minimum 30 reload 60
 standby 1 ip 92.92.92.10
 standby 1 preempt
 standby 1 name PDSN-LAN
 standby 1 track FastEthernet4/2
 standby 1 track FastEthernet4/3
```

```
 standby 1 track FastEthernet4/4
 standby 1 track FastEthernet4/7
 standby 1 track FastEthernet4/9
 standby 1 track FastEthernet4/11
 standby 1 track GigabitEthernet6/1
 standby 1 track Vlan136
 standby 1 track Vlan137
 standby 1 track Vlan127
 standby 1 track Vlan126
 standby 1 track Vlan146
 standby 1 track Vlan147
 standby 1 track Vlan156
 standby 1 track Vlan157
 standby 1 track Vlan166
 standby 1 track Vlan167
 standby 1 track Vlan200
 crypto engine slot 6
!
interface FastEthernet4/3
 ip address 13.0.0.29 255.255.0.0
 standby delay minimum 30 reload 60
 standby 3 ip 13.0.0.30
 standby 3 preempt
 standby 3 name HOME-LAN
 standby 3 track FastEthernet4/2
 standby 3 track FastEthernet4/3
 standby 3 track FastEthernet4/4
 standby 3 track FastEthernet4/7
 standby 3 track FastEthernet4/9
 standby 3 track FastEthernet4/11
 standby 3 track GigabitEthernet6/1
 standby 3 track Vlan136
 standby 3 track Vlan137
 standby 3 track Vlan127
 standby 3 track Vlan126
 standby 3 track Vlan146
 standby 3 track Vlan147
 standby 3 track Vlan156
 standby 3 track Vlan157
 standby 3 track Vlan166
 standby 3 track Vlan167
 standby 3 track Vlan200
crypto engine slot 6
!
interface FastEthernet4/4
 ip address 12.0.0.29 255.255.255.0
 duplex half
 standby delay minimum 30 reload 60
 standby 2 ip 12.0.0.30
 standby 2 preempt
 standby 2 name HOME-LAN-2
 standby 2 track FastEthernet4/2
 standby 2 track FastEthernet4/3
 standby 2 track FastEthernet4/4
 standby 2 track FastEthernet4/7
 standby 2 track FastEthernet4/9
 standby 2 track FastEthernet4/11
 standby 2 track GigabitEthernet6/1
 standby 2 track Vlan136
 standby 2 track Vlan137
 standby 2 track Vlan127
 standby 2 track Vlan126
 standby 2 track Vlan146
 standby 2 track Vlan147
```

```
 standby 2 track Vlan156
 standby 2 track Vlan157
 standby 2 track Vlan166
 standby 2 track Vlan167
 standby 2 track Vlan200
crypto engine slot 6
!
interface FastEthernet4/5
 switchport
 switchport access vlan 137
 switchport mode access
 no ip address
!
interface FastEthernet4/6
 switchport
 switchport access vlan 127
 switchport mode access
 no ip address
 speed 100
 duplex half
!
interface FastEthernet4/7
 ip address 14.0.0.29 255.255.255.0
 standby delay minimum 30 reload 60
 standby 4 ip 14.0.0.30
 standby 4 preempt
 standby 4 name HOME-LAN-4
 standby 4 track FastEthernet4/2
 standby 4 track FastEthernet4/3
 standby 4 track FastEthernet4/4
 standby 4 track FastEthernet4/7
 standby 4 track FastEthernet4/9
 standby 4 track FastEthernet4/11
 standby 4 track Vlan136
 standby 4 track Vlan137
 standby 4 track Vlan127
 standby 4 track Vlan126
 standby 4 track GigabitEthernet6/1
 standby 4 track Vlan146
 standby 4 track Vlan147
 standby 4 track Vlan156
 standby 4 track Vlan157
 standby 4 track Vlan166
 standby 4 track Vlan167
 standby 4 track Vlan200
crypto engine slot 6
!
interface FastEthernet4/8
 switchport
 switchport access vlan 147
 switchport mode access
 no ip address
!
interface FastEthernet4/9
 ip address 15.0.0.29 255.255.255.0
 standby delay minimum 30 reload 60
 standby 5 ip 15.0.0.30
 standby 5 preempt
 standby 5 name HOME-LAN-5
 standby 5 track FastEthernet4/2
 standby 5 track FastEthernet4/3
 standby 5 track FastEthernet4/4
 standby 5 track FastEthernet4/7
 standby 5 track FastEthernet4/9
```

```
 standby 5 track FastEthernet4/11
 standby 5 track Vlan136
 standby 5 track Vlan137
 standby 5 track Vlan127
 standby 5 track Vlan126
 standby 5 track GigabitEthernet6/1
 standby 5 track Vlan146
 standby 5 track Vlan147
 standby 5 track Vlan156
 standby 5 track Vlan157
 standby 5 track Vlan166
 standby 5 track Vlan167
 standby 5 track Vlan200
crypto engine slot 6
!
interface FastEthernet4/10
 switchport
 switchport access vlan 157
 switchport mode access
 no ip address
!
interface FastEthernet4/11
 ip address 16.0.0.29 255.255.255.0
 standby delay minimum 30 reload 60
 standby 6 ip 16.0.0.30
 standby 6 preempt
 standby 6 name HOME-LAN-6
 standby 6 track FastEthernet4/2
 standby 6 track FastEthernet4/3
 standby 6 track FastEthernet4/4
 standby 6 track FastEthernet4/7
 standby 6 track FastEthernet4/9
 standby 6 track FastEthernet4/11
 standby 6 track Vlan136
 standby 6 track Vlan137
 standby 6 track Vlan127
 standby 6 track Vlan126
 standby 6 track GigabitEthernet6/1
 standby 6 track Vlan146
 standby 6 track Vlan147
 standby 6 track Vlan156
 standby 6 track Vlan157
 standby 6 track Vlan166
 standby 6 track Vlan167
 standby 6 track Vlan200
crypto engine slot 6
!
interface FastEthernet4/12
 switchport
 switchport access vlan 167
 switchport mode access
 no ip address
!
interface GigabitEthernet6/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 126,136,146,156,166
 switchport mode trunk
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet6/2
```

```
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan none
 switchport mode trunk
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan126
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha2
 ip address 126.0.0.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA2
 no mop enabled
 crypto map testmap1 ssp 1
 crypto engine slot 6
!
interface Vlan127
 description internal vlan to HA2
 ip vrf forwarding vrf-ha2
 ip address 6.0.0.1 255.255.0.0
 standby 12 ip 6.0.0.5
 standby 12 preempt
 standby 12 name INTERNAL_VLAN_HA2
 standby 12 track FastEthernet4/2
 standby 12 track FastEthernet4/3
 standby 12 track FastEthernet4/4
 standby 12 track FastEthernet4/7
 standby 12 track FastEthernet4/9
 standby 12 track FastEthernet4/11
 standby 12 track Vlan136
 standby 12 track Vlan137
 standby 12 track Vlan127
 standby 12 track Vlan126
 standby 12 track GigabitEthernet6/1
 standby 12 track Vlan146
 standby 12 track Vlan147
 standby 12 track Vlan156
 standby 12 track Vlan157
 standby 12 track Vlan166
 standby 12 track Vlan167
 standby 12 track Vlan200
!
interface Vlan136
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha3
 ip address 136.0.0.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA3
 no mop enabled
 crypto map testmap ssp 1
 crypto engine slot 6
!
interface Vlan137
 description internal vlan to HA3
 ip vrf forwarding vrf-ha3
 ip address 7.0.0.1 255.255.0.0
 standby 13 ip 7.0.0.5
```

```
 standby 13 preempt
 standby 13 name INTERNAL_VLAN_HA3
 standby 13 track FastEthernet4/2
 standby 13 track FastEthernet4/3
 standby 13 track FastEthernet4/4
 standby 13 track FastEthernet4/7
 standby 13 track FastEthernet4/9
 standby 13 track FastEthernet4/11
 standby 13 track Vlan136
 standby 13 track Vlan137
 standby 13 track Vlan127
 standby 13 track Vlan126
 standby 13 track GigabitEthernet6/1
 standby 13 track Vlan146
 standby 13 track Vlan147
 standby 13 track Vlan156
 standby 13 track Vlan157
 standby 13 track Vlan166
 standby 13 track Vlan167
 standby 13 track Vlan200
!
interface Vlan146
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha4
 ip address 146.0.0.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA4
 no mop enabled
 crypto map testmap4 ssp 1
 crypto engine slot 6
!
interface Vlan147
 description internal vlan to HA4
 ip vrf forwarding vrf-ha4
 ip address 8.0.0.1 255.255.0.0
 standby 14 ip 8.0.0.5
 standby 14 preempt
 standby 14 name INTERNAL_VLAN_HA4
 standby 14 track FastEthernet4/2
 standby 14 track FastEthernet4/3
 standby 14 track FastEthernet4/4
 standby 14 track FastEthernet4/7
 standby 14 track FastEthernet4/9
 standby 14 track FastEthernet4/11
 standby 14 track Vlan136
 standby 14 track Vlan137
 standby 14 track Vlan127
 standby 14 track Vlan126
 standby 14 track GigabitEthernet6/1
 standby 14 track Vlan146
 standby 14 track Vlan147
 standby 14 track Vlan156
 standby 14 track Vlan157
 standby 14 track Vlan166
 standby 14 track Vlan167
 standby 14 track Vlan200
!
interface Vlan156
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha5
 ip address 156.0.0.1 255.255.255.0
```

```
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA5
 no mop enabled
 crypto map testmap5 ssp 1
 crypto engine slot 6
!
interface Vlan157
 description internal vlan to HA5
 ip vrf forwarding vrf-ha5
 ip address 9.0.0.1 255.255.0.0
 standby 15 ip 9.0.0.5
 standby 15 preempt
 standby 15 name INTERNAL_VLAN_HA5
 standby 15 track FastEthernet4/2
 standby 15 track FastEthernet4/3
 standby 15 track FastEthernet4/4
 standby 15 track FastEthernet4/7
 standby 15 track FastEthernet4/9
 standby 15 track FastEthernet4/11
 standby 15 track Vlan136
 standby 15 track Vlan137
 standby 15 track Vlan127
 standby 15 track Vlan126
 standby 15 track GigabitEthernet6/1
 standby 15 track Vlan146
 standby 15 track Vlan147
 standby 15 track Vlan156
 standby 15 track Vlan157
 standby 15 track Vlan166
 standby 15 track Vlan167
 standby 15 track Vlan200
!
interface Vlan166
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha6
 ip address 166.0.0.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA6
 no mop enabled
 crypto map testmap6 ssp 1
 crypto engine slot 6
!
interface Vlan167
 description internal vlan to HA6
 ip vrf forwarding vrf-ha6
 ip address 10.0.0.1 255.255.0.0
 standby 16 ip 10.0.0.5
 standby 16 preempt
 standby 16 name INTERNAL_VLAN_HA6
 standby 16 track FastEthernet4/2
 standby 16 track FastEthernet4/3
 standby 16 track FastEthernet4/4
 standby 16 track FastEthernet4/7
 standby 16 track FastEthernet4/9
 standby 16 track FastEthernet4/11
 standby 16 track Vlan136
 standby 16 track Vlan137
 standby 16 track Vlan127
 standby 16 track Vlan126
 standby 16 track GigabitEthernet6/1
 standby 16 track Vlan146
```

```
 standby 16 track Vlan147
 standby 16 track Vlan156
 standby 16 track Vlan157
 standby 16 track Vlan166
 standby 16 track Vlan167
 standby 16 track Vlan200
!
interface vlan 200
 ip address 200.0.0.2 255.0.0.0
 standby 250 ip 200.0.0.3
 standby 250 preempt
 standby 250 name NON_IPSEC_VLAN
 standby 250 track FastEthernet4/2
 standby 250 track FastEthernet4/3
 standby 250 track FastEthernet4/4
 standby 250 track FastEthernet4/7
 standby 250 track FastEthernet4/9
 standby 250 track FastEthernet4/11
 standby 250 track Vlan136
 standby 250 track Vlan137
 standby 250 track Vlan127
 standby 250 track Vlan126
 standby 250 track GigabitEthernet6/1
 standby 250 track Vlan146
 standby 250 track Vlan147
 standby 250 track Vlan156
 standby 250 track Vlan157
 standby 250 track Vlan166
 standby 250 track Vlan167
!
ip route vrf vrf-ha2 92.92.92.0 255.255.255.0 Vlan126 92.92.92.1 global
ip route vrf vrf-ha3 92.92.92.0 255.255.255.0 Vlan136 92.92.92.1 global
ip route vrf vrf-ha4 92.92.92.0 255.255.255.0 Vlan146 92.92.92.1 global
ip route vrf vrf-ha5 92.92.92.0 255.255.255.0 Vlan156 92.92.92.1 global
ip route vrf vrf-ha6 92.92.92.0 255.255.255.0 Vlan166 92.92.92.1 global
!
access-list 121 permit ip host 12.0.0.30 host 92.92.92.1
access-list 121 remark Access List for HA2
access-list 131 permit ip host 13.0.0.30 host 92.92.92.1
access-list 131 remark Access List for HA3
access-list 141 permit ip host 14.0.0.30 host 92.92.92.1
access-list 141 remark Access List for HA4
access-list 151 permit ip host 15.0.0.30 host 92.92.92.1
access-list 151 remark Access List for HA5
access-list 161 permit ip host 16.0.0.30 host 92.92.92.1
access-list 161 remark Access List for HA6
access-list 2000 permit udp any any eq mobile-ip
access-list 2000 permit ipinip any any
access-list 2001 permit ip 95.95.95.0 0.0.0.255 host 120.0.0.30
access-list 2002 permit ip 96.96.96.0 0.0.0.255 host 130.0.0.30
access-list 2003 permit ip 97.97.97.0 0.0.0.255 host 140.0.0.30
access-list 2004 permit ip 98.98.98.0 0.0.0.255 host 150.0.0.30
access-list 2005 permit ip 99.99.99.0 0.0.0.255 host 160.0.0.30
!
arp vrf vrf-ha6 10.0.0.10 0000.0c07.ac32 ARPA
arp vrf vrf-ha4 8.0.0.10 0000.0c07.ac1e ARPA
arp vrf vrf-ha5 9.0.0.10 0000.0c07.ac28 ARPA
arp vrf vrf-ha2 6.0.0.10 0000.0c07.ac0a ARPA
arp vrf vrf-ha3 7.0.0.10 0000.0c07.ac14 ARPA
!
route-map RRQ-HA5 permit 10
 match ip address 2000
 set ip next-hop 9.0.0.10
!
```

```
route-map RRQ-HA4 permit 10
 match ip address 2000
 set ip next-hop 8.0.0.10
!
route-map RRQ-HA6 permit 10
 match ip address 2000
 set ip next-hop 10.0.0.10
!
route-map RRQ-HA3 permit 10
 match ip address 2000
 set ip next-hop 7.0.0.10
!
route-map RRQ-HA2 permit 10
 match ip address 2000
 set ip next-hop 6.0.0.10
!
route-map RRQ-HA10 permit 10
 match ip address 2001
 continue 11
 set ip next-hop 200.0.0.5
!
route-map RRQ-HA10 permit 11
 match ip address 2002
 continue 12
 set ip next-hop 200.0.0.15
!
route-map RRQ-HA10 permit 12
 match ip address 2003
 continue 13
 set ip next-hop 200.0.0.25
!
route-map RRQ-HA10 permit 13
 match ip address 2004
 continue 14
 set ip next-hop 200.0.0.35
!
route-map RRQ-HA10 permit 14
 match ip address 2005
 set ip next-hop 200.0.0.45
```

### SUP Configuration - Switch 2:

```
ip vrf vrf-ha2
 rd 2000:1
 route-target export 2000:1
 route-target import 2000:1
!
ip vrf vrf-ha3
 rd 1000:1
 route-target export 1000:1
 route-target import 1000:1
!
ip vrf vrf-ha4
 rd 4000:1
 route-target export 4000:1
 route-target import 4000:1
!
ip vrf vrf-ha5
 rd 5000:1
 route-target export 5000:1
 route-target import 5000:1
!
```

```
ip vrf vrf-ha6
 rd 6000:1
 route-target export 6000:1
 route-target import 6000:1
!
ssp group 1
 remote 13.0.0.29
 redundancy PDSN-LAN
 redundancy HOME-LAN
 redundancy INTERNAL_VLAN_HA3
 redundancy HOME-LAN-2
 redundancy INTERNAL_VLAN_HA2
 redundancy HOME-LAN-4
 redundancy HOME-LAN-5
 redundancy HOME-LAN-6
 redundancy INTERNAL_VLAN_HA4
 redundancy INTERNAL_VLAN_HA5
 redundancy INTERNAL_VLAN_HA6
 port 4098
!
crypto keyring key0
  pre-shared-key address 92.92.92.1 key cisco
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 60000
crypto isakmp ssp 1
!
crypto isakmp profile prof1
   vrf vrf-ha2
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 12.0.0.30
crypto isakmp profile prof2
   vrf vrf-ha3
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 13.0.0.30
crypto isakmp profile prof4
   vrf vrf-ha4
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 14.0.0.30
crypto isakmp profile prof5
   vrf vrf-ha5
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 15.0.0.30
crypto isakmp profile prof6
   vrf vrf-ha6
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 16.0.0.30
!
crypto ipsec transform-set mobile-set1 esp-des esp-sha-hmac
!
crypto map testmap local-address FastEthernet2/3
crypto map testmap 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof2
 match address 131
!
crypto map testmap1 local-address FastEthernet2/5
```

```
crypto map testmap1 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof1
 match address 121
!
crypto map testmap4 local-address FastEthernet2/7
crypto map testmap4 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof4
 match address 141
!
crypto map testmap5 local-address FastEthernet2/9
crypto map testmap5 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof5
 match address 151
!
crypto map testmap6 local-address FastEthernet2/11
crypto map testmap6 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof6
 match address 161
!
crypto engine mode vrf
!
interface FastEthernet2/2
 ip address 92.92.92.11 255.255.0.0
 ip policy route-map RRQ-HA10
 speed 100
 duplex full
 standby delay minimum 30 reload 60
 standby 1 ip 92.92.92.10
 standby 1 preempt
 standby 1 name PDSN-LAN
 standby 1 track FastEthernet2/2
 standby 1 track FastEthernet2/3
 standby 1 track FastEthernet2/5
 standby 1 track FastEthernet2/7
 standby 1 track FastEthernet2/9
 standby 1 track FastEthernet2/11
 standby 1 track GigabitEthernet4/1
 standby 1 track Vlan136
 standby 1 track Vlan137
 standby 1 track Vlan127
 standby 1 track Vlan126
 standby 1 track Vlan146
 standby 1 track Vlan156
 standby 1 track Vlan157
 standby 1 track Vlan166
 standby 1 track Vlan167
 standby 1 track Vlan147
 standby 1 track Vlan200
 crypto engine slot 4
!
interface FastEthernet2/3
 ip address 13.0.0.31 255.255.0.0
 standby delay minimum 30 reload 60
 standby 3 ip 13.0.0.30
 standby 3 preempt
 standby 3 name HOME-LAN
```

```
 standby 3 track FastEthernet2/2
 standby 3 track FastEthernet2/3
 standby 3 track FastEthernet2/5
 standby 3 track FastEthernet2/7
 standby 3 track FastEthernet2/9
 standby 3 track FastEthernet2/11
 standby 3 track GigabitEthernet4/1
 standby 3 track Vlan136
 standby 3 track Vlan137
 standby 3 track Vlan127
 standby 3 track Vlan126
 standby 3 track Vlan146
 standby 3 track Vlan156
 standby 3 track Vlan157
 standby 3 track Vlan166
 standby 3 track Vlan167
 standby 3 track Vlan147
 standby 3 track Vlan200
crypto engine slot 4
!
interface FastEthernet2/4
 switchport
 switchport access vlan 137
 switchport mode access
 no ip address
!
interface FastEthernet2/5
 ip address 12.0.0.31 255.255.0.0
 standby delay minimum 30 reload 60
 standby 2 ip 12.0.0.30
 standby 2 preempt
 standby 2 name HOME-LAN-2
 standby 2 track FastEthernet2/2
 standby 2 track FastEthernet2/3
 standby 2 track FastEthernet2/5
 standby 2 track FastEthernet2/7
 standby 2 track FastEthernet2/9
 standby 2 track FastEthernet2/11
 standby 2 track GigabitEthernet4/1
 standby 2 track Vlan136
 standby 2 track Vlan137
 standby 2 track Vlan127
 standby 2 track Vlan126
 standby 2 track Vlan146
 standby 2 track Vlan156
 standby 2 track Vlan157
 standby 2 track Vlan166
 standby 2 track Vlan167
 standby 2 track Vlan147
 standby 2 track Vlan200
 crypto engine slot 4
!
interface FastEthernet2/6
 switchport
 switchport access vlan 127
 switchport mode access
 no ip address
!
interface FastEthernet2/7
 ip address 14.0.0.31 255.255.0.0
 standby delay minimum 30 reload 60
 standby 4 ip 14.0.0.30
 standby 4 preempt
 standby 4 name HOME-LAN-4
```

```
 standby 4 track FastEthernet2/2
 standby 4 track FastEthernet2/3
 standby 4 track FastEthernet2/5
 standby 4 track FastEthernet2/7
 standby 4 track FastEthernet2/9
 standby 4 track FastEthernet2/11
 standby 4 track Vlan136
 standby 4 track Vlan137
 standby 4 track Vlan127
 standby 4 track Vlan126
 standby 4 track GigabitEthernet4/1
 standby 4 track Vlan146
 standby 4 track Vlan156
 standby 4 track Vlan157
 standby 4 track Vlan166
 standby 4 track Vlan167
 standby 4 track Vlan147
 standby 4 track Vlan200
crypto engine slot 4
!
interface FastEthernet2/8
 switchport
 switchport access vlan 147
 switchport mode access
 no ip address
!
interface FastEthernet2/9
 ip address 15.0.0.31 255.255.0.0
 standby delay minimum 30 reload 60
 standby 5 ip 15.0.0.30
 standby 5 preempt
 standby 5 name HOME-LAN-5
 standby 5 track FastEthernet2/2
 standby 5 track FastEthernet2/3
 standby 5 track FastEthernet2/5
 standby 5 track FastEthernet2/7
 standby 5 track FastEthernet2/9
 standby 5 track FastEthernet2/11
 standby 5 track Vlan136
 standby 5 track Vlan137
 standby 5 track Vlan127
 standby 5 track Vlan126
 standby 5 track GigabitEthernet4/1
 standby 5 track Vlan146
 standby 5 track Vlan156
 standby 5 track Vlan157
 standby 5 track Vlan166
 standby 5 track Vlan167
 standby 5 track Vlan147
 standby 5 track Vlan200
crypto engine slot 4
!
interface FastEthernet2/10
 switchport
 switchport access vlan 157
 switchport mode access
 no ip address
!
interface FastEthernet2/11
 ip address 16.0.0.31 255.255.0.0
 standby delay minimum 30 reload 60
 standby 6 ip 16.0.0.30
 standby 6 preempt
 standby 6 name HOME-LAN-6
```

```
 standby 6 track FastEthernet2/2
 standby 6 track FastEthernet2/3
 standby 6 track FastEthernet2/5
 standby 6 track FastEthernet2/7
 standby 6 track FastEthernet2/9
 standby 6 track FastEthernet2/11
 standby 6 track Vlan136
 standby 6 track Vlan137
 standby 6 track Vlan127
 standby 6 track Vlan126
 standby 6 track GigabitEthernet4/1
 standby 6 track Vlan146
 standby 6 track Vlan156
 standby 6 track Vlan157
 standby 6 track Vlan166
 standby 6 track Vlan167
 standby 6 track Vlan147
 standby 6 track Vlan200
 crypto engine slot 4
!
interface FastEthernet2/12
 switchport
 switchport access vlan 167
 switchport mode access
 no ip address
!
interface GigabitEthernet4/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 126,136,146,156,166
 switchport mode trunk
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet4/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan none
 switchport mode trunk
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan126
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha2
 ip address 126.0.0.2 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA2
 no mop enabled
 crypto map testmap1 ssp 1
 crypto engine slot 4
!
interface Vlan127
 description internal vlan to HA2
 ip vrf forwarding vrf-ha2
 ip address 6.0.0.2 255.255.0.0
 standby 12 ip 6.0.0.5
 standby 12 preempt
```

```
 standby 12 name INTERNAL_VLAN_HA2
 standby 12 track FastEthernet2/2
 standby 12 track FastEthernet2/3
 standby 12 track FastEthernet2/5
 standby 12 track FastEthernet2/7
 standby 12 track FastEthernet2/9
 standby 12 track FastEthernet2/11
 standby 12 track Vlan136
 standby 12 track Vlan137
 standby 12 track Vlan127
 standby 12 track Vlan126
 standby 12 track GigabitEthernet4/1
 standby 12 track Vlan146
 standby 12 track Vlan156
 standby 12 track Vlan157
 standby 12 track Vlan166
 standby 12 track Vlan167
 standby 12 track Vlan147
 standby 12 track Vlan200
!
interface Vlan136
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha3
 ip address 136.0.0.2 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA3
 no mop enabled
 crypto map testmap ssp 1
 crypto engine slot 4
!
interface Vlan137
 description internal vlan to HA3
 ip vrf forwarding vrf-ha3
 ip address 7.0.0.2 255.255.0.0
 standby 13 ip 7.0.0.5
 standby 13 preempt
 standby 13 name INTERNAL_VLAN_HA3
 standby 13 track FastEthernet2/2
 standby 13 track FastEthernet2/3
 standby 13 track FastEthernet2/5
 standby 13 track FastEthernet2/7
 standby 13 track FastEthernet2/9
 standby 13 track FastEthernet2/11
 standby 13 track Vlan136
 standby 13 track Vlan137
 standby 13 track Vlan127
 standby 13 track Vlan126
 standby 13 track GigabitEthernet4/1
 standby 13 track Vlan146
 standby 13 track Vlan156
 standby 13 track Vlan157
 standby 13 track Vlan166
 standby 13 track Vlan167
 standby 13 track Vlan147
 standby 13 track Vlan200
!
interface Vlan146
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha4
 ip address 146.0.0.2 255.0.0.0
 no ip redirects
```

```
 no ip unreachables
 ip policy route-map RRQ-HA4
 no mop enabled
 crypto map testmap4 ssp 1
 crypto engine slot 4
!
interface Vlan147
 description internal vlan to HA4
 ip vrf forwarding vrf-ha4
 ip address 8.0.0.2 255.255.0.0
 standby 14 ip 8.0.0.5
 standby 14 preempt
 standby 14 name INTERNAL_VLAN_HA4
 standby 14 track FastEthernet2/2
 standby 14 track FastEthernet2/3
 standby 14 track FastEthernet2/5
 standby 14 track FastEthernet2/7
 standby 14 track FastEthernet2/9
 standby 14 track FastEthernet2/11
 standby 14 track Vlan136
 standby 14 track Vlan137
 standby 14 track Vlan127
 standby 14 track Vlan126
 standby 14 track GigabitEthernet4/1
 standby 14 track Vlan146
 standby 14 track Vlan156
 standby 14 track Vlan157
 standby 14 track Vlan166
 standby 14 track Vlan167
 standby 14 track Vlan147
 standby 14 track Vlan200
!
interface Vlan156
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha5
 ip address 156.0.0.2 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA5
 no mop enabled
 crypto map testmap5 ssp 1
 crypto engine slot 4
!
interface Vlan157
 description internal vlan to HA5
 ip vrf forwarding vrf-ha5
 ip address 9.0.0.2 255.255.0.0
 standby 15 ip 9.0.0.5
 standby 15 preempt
 standby 15 name INTERNAL_VLAN_HA5
 standby 15 track FastEthernet2/2
 standby 15 track FastEthernet2/3
 standby 15 track FastEthernet2/5
 standby 15 track FastEthernet2/7
 standby 15 track FastEthernet2/9
 standby 15 track FastEthernet2/11
 standby 15 track Vlan136
 standby 15 track Vlan137
 standby 15 track Vlan127
 standby 15 track Vlan126
 standby 15 track GigabitEthernet4/1
 standby 15 track Vlan146
 standby 15 track Vlan156
```

```
 standby 15 track Vlan157
 standby 15 track Vlan166
 standby 15 track Vlan167
 standby 15 track Vlan147
 standby 15 track Vlan200
!
interface Vlan166
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha6
 ip address 166.0.0.2 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA6
 no mop enabled
 crypto map testmap6 ssp 1
 crypto engine slot 4
!
interface Vlan167
 description internal vlan to HA2
 ip vrf forwarding vrf-ha6
 ip address 10.0.0.2 255.255.0.0
 standby 16 ip 10.0.0.5
 standby 16 preempt
 standby 16 name INTERNAL_VLAN_HA6
 standby 16 track FastEthernet2/2
 standby 16 track FastEthernet2/3
 standby 16 track FastEthernet2/5
 standby 16 track FastEthernet2/7
 standby 16 track FastEthernet2/9
 standby 16 track FastEthernet2/11
 standby 16 track Vlan136
 standby 16 track Vlan137
 standby 16 track Vlan127
 standby 16 track Vlan126
 standby 16 track GigabitEthernet4/1
 standby 16 track Vlan146
 standby 16 track Vlan156
 standby 16 track Vlan157
 standby 16 track Vlan166
 standby 16 track Vlan167
 standby 16 track Vlan147
 standby 16 track Vlan200
!
interface vlan 200
 ip address 200.0.0.1 255.0.0.0
 standby 250 ip 200.0.0.3
 standby 250 preempt
 standby 250 name NON_IPSEC_VLAN
 standby 250 track FastEthernet2/2
 standby 250 track FastEthernet2/3
 standby 250 track FastEthernet2/5
 standby 250 track FastEthernet2/7
 standby 250 track FastEthernet2/9
 standby 250 track FastEthernet2/11
 standby 250 track Vlan136
 standby 250 track Vlan137
 standby 250 track Vlan127
 standby 250 track Vlan126
 standby 250 track GigabitEthernet4/1
 standby 250 track Vlan146
 standby 250 track Vlan156
 standby 250 track Vlan157
 standby 250 track Vlan166
```

```
 standby 250 track Vlan167
 standby 250 track Vlan147

ip route vrf vrf-ha2 92.92.92.0 255.255.255.0 Vlan126 92.92.92.1 global
ip route vrf vrf-ha3 92.92.92.0 255.255.255.0 Vlan136 92.92.92.1 global
ip route vrf vrf-ha4 92.92.92.0 255.255.255.0 Vlan146 92.92.92.1 global
ip route vrf vrf-ha5 92.92.92.0 255.255.255.0 Vlan156 92.92.92.1 global
ip route vrf vrf-ha6 92.92.92.0 255.255.255.0 Vlan166 92.92.92.1 global
!
access-list 121 permit ip host 12.0.0.30 host 92.92.92.1
access-list 121 remark Access List for HA2
access-list 131 permit ip host 13.0.0.30 host 92.92.92.1
access-list 131 remark Access List for HA3
access-list 141 permit ip host 14.0.0.30 host 92.92.92.1
access-list 141 remark Access List for HA4
access-list 151 permit ip host 15.0.0.30 host 92.92.92.1
access-list 151 remark Access List for HA5
access-list 161 permit ip host 16.0.0.30 host 92.92.92.1
access-list 161 remark Access List for HA6
access-list 2000 permit udp any any eq mobile-ip
access-list 2000 permit ipinip any any
access-list 2001 permit ip 95.95.95.0 0.0.0.255 host 120.0.0.30
access-list 2002 permit ip 96.96.96.0 0.0.0.255 host 130.0.0.30
access-list 2003 permit ip 97.97.97.0 0.0.0.255 host 140.0.0.30
access-list 2004 permit ip 98.98.98.0 0.0.0.255 host 150.0.0.30
access-list 2005 permit ip 99.99.99.0 0.0.0.255 host 160.0.0.30
!
arp vrf vrf-ha6 10.0.0.10 0000.0c07.ac32 ARPA
arp vrf vrf-ha4 8.0.0.10 0000.0c07.ac1e ARPA
arp vrf vrf-ha5 9.0.0.10 0000.0c07.ac28 ARPA
arp vrf vrf-ha2 6.0.0.10 0000.0c07.ac0a ARPA
arp vrf vrf-ha3 7.0.0.10 0000.0c07.ac14 ARPA
!
route-map RRQ-HA5 permit 10
 match ip address 2000
 set ip next-hop 9.0.0.10
!
route-map RRQ-HA4 permit 10
 match ip address 2000
 set ip next-hop 8.0.0.10
!
route-map RRQ-HA6 permit 10
 match ip address 2000
 set ip next-hop 10.0.0.10
!
route-map RRQ-HA3 permit 10
 match ip address 2000
 set ip next-hop 7.0.0.10
!
route-map RRQ-HA2 permit 10
 match ip address 2000
 set ip next-hop 6.0.0.10
!
route-map RRQ-HA10 permit 10
 match ip address 2001
 continue 11
 set ip next-hop 200.0.0.5
!
route-map RRQ-HA10 permit 11
 match ip address 2002
 continue 12
 set ip next-hop 200.0.0.15
!
route-map RRQ-HA10 permit 12
```

```
 match ip address 2003
 continue 13
 set ip next-hop 200.0.0.25
!
route-map RRQ-HA10 permit 13
 match ip address 2004
 continue 14
 set ip next-hop 200.0.0.35
!
route-map RRQ-HA10 permit 14
 match ip address 2005
 set ip next-hop 200.0.0.45
```

## HA Configuration - Switch 1:

### HA1:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 12.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.126
 encapsulation dot1Q 126
 ip address 126.0.0.82 255.255.255.0
!
interface GigabitEthernet0/0.127
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 127
 ip address 6.0.0.3 255.255.255.0
 standby 10 ip 6.0.0.10
 standby 10 preempt
 standby 10 name HSRP_HA_HA2
 standby 10 track GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.4 255.0.0.0
 no snmp trap link-status
 standby 200 ip 200.0.0.5
 standby 200 preempt
 standby 200 track GigabitEthernet0/0.127
!
router mobile
!
ip local pool ha-pool2 10.1.2.1 10.1.2.255
ip route 92.92.92.1 255.255.255.255 6.0.0.5
ip route 95.95.95.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA2 virtual-network address 12.0.0.30 mode
active-standby
ip mobile virtual-network 12.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool2 virtual-network 12.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 6.0.0.4 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

**HA2:**

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 13.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.136
 encapsulation dot1Q 136
 ip address 136.0.0.83 255.255.255.0
!
interface GigabitEthernet0/0.137
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 137
 ip address 7.0.0.3 255.255.255.0
 standby 20 ip 7.0.0.10
 standby 20 preempt
 standby 20 name HSRP_HA_HA3
 standby 20 name GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.14 255.0.0.0
 no snmp trap link-status
 standby 201 ip 200.0.0.15
 standby 201 preempt
 standby 201 track GigabitEthernet0/0.137
!
router mobile
!
ip local pool ha-pool3 10.1.3.1 10.1.3.255
ip route 92.92.92.1 255.255.255.255 7.0.0.5
ip route 96.96.96.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA3 virtual-network address 13.0.0.30 mode
active-standby
ip mobile virtual-network 13.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool3 virtual-network 13.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 7.0.0.4 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

**HA3:**

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 14.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.146
 encapsulation dot1Q 146
 ip address 146.0.0.82 255.255.255.0
!
interface GigabitEthernet0/0.147
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 147
 ip address 8.0.0.3 255.255.255.0
 standby 30 ip 8.0.0.10
 standby 30 preempt
 standby 30 name HSRP_HA_HA4
```

```
 standby 30 name GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.24 255.0.0.0
 no snmp trap link-status
 standby 202 ip 200.0.0.25
 standby 202 preempt
 standby 202 track GigabitEthernet0/0.147
!
router mobile
!
ip local pool ha-pool4 10.1.4.1 10.1.4.255
ip route 92.92.92.1 255.255.255.255 8.0.0.5
ip route 97.97.97.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA4 virtual-network address 14.0.0.30 mode
active-standby
ip mobile virtual-network 13.0.0.10 255.255.255.255
ip mobile virtual-network 14.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool4 virtual-network 14.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 8.0.0.4 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

**HA4:**

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 15.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.156
 encapsulation dot1Q 156
 ip address 156.0.0.82 255.255.255.0
!
interface GigabitEthernet0/0.157
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 157
 ip address 9.0.0.3 255.255.255.0
 standby 40 ip 9.0.0.10
 standby 40 preempt
 standby 40 name HSRP_HA_HA5
 standby 40 name GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.34 255.0.0.0
 no snmp trap link-status
 standby 203 ip 200.0.0.35
 standby 203 preempt
 standby 203 track GigabitEthernet0/0.157
!
router mobile
!
ip local pool ha-pool5 10.1.5.1 10.1.5.255
ip route 92.92.92.1 255.255.255.255 9.0.0.5
ip route 98.98.98.0 255.255.255.0 200.0.0.3
!
```

```
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA5 virtual-network address 15.0.0.30 mode
active-standby
ip mobile virtual-network 15.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool5 virtual-network 15.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 9.0.0.4 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

**HA5:**

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 16.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.166
 encapsulation dot1Q 166
 ip address 166.0.0.82 255.255.255.0
!
interface GigabitEthernet0/0.167
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 167
 ip address 10.0.0.3 255.255.255.0
 standby 50 ip 10.0.0.10
 standby 50 preempt
 standby 50 name HSRP_HA_HA6
 standby 50 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.44 255.0.0.0
 no snmp trap link-status
 standby 204 ip 200.0.0.45
 standby 204 preempt
 standby 204 track GigabitEthernet0/0.167
!
router mobile
!
ip local pool ha-pool6 10.1.6.1 10.1.6.255
ip route 92.92.92.1 255.255.255.255 10.0.0.5
ip route 99.99.99.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA6 virtual-network address 16.0.0.30 mode
active-standby
ip mobile virtual-network 16.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool6 virtual-network 16.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 10.0.0.4 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

## HA Configuration - Switch 2:

### HA1:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 12.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.126
 encapsulation dot1Q 126
 ip address 126.0.0.32 255.255.255.0
!
interface GigabitEthernet0/0.127
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 127
 ip address 6.0.0.4 255.255.255.0
 standby 10 ip 6.0.0.10
 standby 10 preempt
 standby 10 name HSRP_HA_HA2
 standby 10 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.6 255.0.0.0
 no snmp trap link-status
 standby 200 ip 200.0.0.5
 standby 200 preempt
 standby 200 track GigabitEthernet0/0.127
!
router mobile
!
ip local pool ha-pool2 10.1.2.1 10.1.2.255
ip route 92.92.92.1 255.255.255.255 6.0.0.5
ip route 95.95.95.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA2 virtual-network address 12.0.0.30 mode
active-standby
ip mobile virtual-network 12.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool2 virtual-network 12.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 6.0.0.3 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

### HA2:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 13.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.136
 encapsulation dot1Q 136
 ip address 136.0.0.33 255.255.255.0
!
interface GigabitEthernet0/0.137
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 137
 ip address 7.0.0.4 255.255.255.0
 standby 20 ip 7.0.0.10
 standby 20 preempt
```

```
 standby 20 name HSRP_HA_HA3
 standby 20 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.16 255.0.0.0
 no snmp trap link-status
 standby 201 ip 200.0.0.15
 standby 201 preempt
 standby 201 track GigabitEthernet0/0.137
!
router mobile
!
ip local pool ha-pool3 10.1.3.1 10.1.3.255
ip route 92.92.92.1 255.255.255.255 7.0.0.5
ip route 96.96.96.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA3 virtual-network address 13.0.0.30 mode
active-standby
ip mobile virtual-network 13.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool3 virtual-network 13.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 7.0.0.3 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

**HA3:**

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 14.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.146
 encapsulation dot1Q 146
 ip address 146.0.0.32 255.255.255.0
!
interface GigabitEthernet0/0.147
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 147
 ip address 8.0.0.4 255.255.255.0
 standby 30 ip 8.0.0.10
 standby 30 preempt
 standby 30 name HSRP_HA_HA4
 standby 30 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.26 255.0.0.0
 no snmp trap link-status
 standby 202 ip 200.0.0.25
 standby 202 preempt
 standby 202 track GigabitEthernet0/0.147
!
router mobile
!
ip local pool ha-pool4 10.1.4.1 10.1.4.255
ip route 92.92.92.1 255.255.255.255 8.0.0.5
ip route 97.97.97.0 255.255.255.0 200.0.0.3
!
```

```
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA4 virtual-network address 14.0.0.30 mode
active-standby
ip mobile virtual-network 14.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool4 virtual-network 14.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 8.0.0.3 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

**HA4:**

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 15.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.156
 encapsulation dot1Q 156
 ip address 156.0.0.32 255.255.255.0
!
interface GigabitEthernet0/0.157
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 157
 ip address 9.0.0.4 255.255.255.0
 standby 40 ip 9.0.0.10
 standby 40 preempt
 standby 40 name HSRP_HA_HA5
 standby 40 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.36 255.0.0.0
 no snmp trap link-status
 standby 203 ip 200.0.0.35
 standby 203 preempt
 standby 203 track GigabitEthernet0/0.157
!
router mobile
!
ip local pool ha-pool5 10.1.5.1 10.1.5.255
ip route 92.92.92.1 255.255.255.255 9.0.0.5
ip route 98.98.98.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA5 virtual-network address 15.0.0.30 mode
active-standby
ip mobile virtual-network 15.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool5 virtual-network 15.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 9.0.0.3 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

**HA5:**

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 16.0.0.30 255.255.255.255
!
```

```
interface GigabitEthernet0/0.166
 encapsulation dot1Q 166
 ip address 166.0.0.32 255.255.255.0
!
interface GigabitEthernet0/0.167
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 167
 ip address 10.0.0.4 255.255.255.0
 standby 50 ip 10.0.0.10
 standby 50 preempt
 standby 50 name HSRP_HA_HA6
 standby 50 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.46 255.0.0.0
 no snmp trap link-status
 standby 204 ip 200.0.0.45
 standby 204 preempt
 standby 204 track GigabitEthernet0/0.167
!
router mobile
!
ip local pool ha-pool6 10.1.6.1 10.1.6.255
ip route 92.92.92.1 255.255.255.255 10.0.0.5
ip route 98.98.98.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA6 virtual-network address 16.0.0.30 mode
active-standby
ip mobile virtual-network 16.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool6 virtual-network 16.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 10.0.0.3 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

CHAPTER 1

# Home Agent Accounting

This chapter discusses concepts related to accounting on the Cisco Mobile Wireless Home Agent, and provides details about how to configure this feature.

This chapter includes the following sections:



## Overview of HA Accounting

This feature is primarily developed to allow the HA to interoperate with the Service Selection Gateway (SSG) in the CMX solution. However, this feature can also be used without SSG interaction.

Release 3.0 supports the following enhancements to the Accounting feature:

- Home Agent Accounting in a Redundant Setup
- Packet count and Byte count in Accounting Records
- Additional Attributes in the Accounting Records
- Additional Accounting Methods—Interim Accounting is Supported.

As byte count and packet count is performed on the HA, this accounting feature does not need the SSG in the network to generate full accounting information.

The HA Accounting feature includes the following activities:

- The HA sends an Accounting Start record when the first binding for a mobile is created.
- The HA sends an Accounting Stop record when the last binding for a mobile is deleted.
- The HA sends an Accounting Update when Handoff occurs .

- Start-stop, and Interim accounting methods are supported.
- When a mobileip registration reply with an error code is sent for an authenticated NAI (if a binding does not exit for the NAI), an accounting stop record is sent.
- If Re-registration fails for an existing binding, a watchdog message is sent with an appropriate reject code for an authenticated NAI.

The following attributes are sent in Accounting Records:

- NAI in Username attribute (1)
- MN IP Address in Framed IP Address attribute (8)
- Home Agent IP Address(26/7, 3gpp2 attribute)
- Care-of-address in Tunnel End Point (66)
- Network Access Server (NAS) IP Address attribute (4)
- Accounting Status Type attribute (40)
- Accounting Session ID (44)
- Accounting Terminate Cause(49) - only in accounting stop
- Accounting Delay Time(41)
- Acct-Input-Octets (42)
- Acct-Output-Octets (43)
- Acct-Input-Packets (47)
- Acct-Output-Packets (48)
- Acct-Input-Gigawords(52)
- Acct-Output-Gigawords(53)
- Registration flags in “mobileip-mn-flags” cisco-avpair attribute
- Vrf name in “mobileip:ip-vrf” cisco-avpair attribute
- “mobileip:mn-reject-code” cisco-avpair attribute (only in accounting-stop and accounting update, when an RRQ is rejected.)

Use the following commands to enable the HA accounting features:

**ip mobile home-agent accounting** *method name*

## Synching Accounting Counters with HA Redundancy Setup

If Home Agent accounting is enabled in a redundant setup along with periodic accounting, accounting counters are periodically synched between the active and standby if the following command is configured:

**ip mobile home-agent** *method* **redundancy** [**virtual-network address** *address*] **periodic-sync**

When you configure the **ip mobile home-agent** *method* **redundancy periodic-sync** command, the byte and packet counts for each binding are synced to the standby unit using an accounting update event, if and only if the byte counts have changed since the last sync. Time-of-the-day accounting is not supported.

Here is an example:

If you configure **aaa accounting update periodic** *60* and **ip mobile home-agent** *method* **redundancy update-periodic**, and open a binding, the following events occur:

- If no data passes through the binding after the binding is opened, the byte counts will not be synced to the standby unit even though the interim accounting records are sent to the AAA server.
- Assume that 500 bytes pass through the binding in either direction before the next interim record is sent. In this case, when the interim record is triggered from the active unit, counters are synched to the standby
- Now, assume that no more data is pumped through the flow before the next interim interval. Now, when the interim record is triggered from the active unit, nothing is synched to the standby unit, as there is nothing new to report.
- At this point, if a switchover happens, the newly active unit will have a count of 500 bytes in/out and 5 packets in/out (assuming 5 packets of 100 bytes each had passed through the binding at step 2) for the binding. After the old active recovers and becomes a standby unit, these counters will be bulk synced to the standby unit.

The Home Agent can notify the RADIUS server of a home agent failover. This is achieved by including the cisco-avpair radius attribute “mobileip-rfswat=1” in RADIUS accounting records. This attribute is included only in the first accounting record of a binding generated after a failover, and if that binding was created before the failover.

For example, when a binding is created, an accounting start is sent for the binding. After a while, the active reloads and the standby takes over. After some time, the standby sends an accounting update to the RADIUS server for the binding. Cisco-avpair radius attribute “mobileip-rfswat=1” is added to this accounting record by the Home Agent.

The command to enable this feature is:

ip mobile home-agent redundancy *group* virtual-network address *HA address* swact-notification

## Basic Accounting Messages

The Cisco Mobile Wireless Home Agent supports the Cisco Service Selection Gateway (SSG). In this release, the HA sends only three accounting messages without statistics information. The SSG is designed and deployed in such a way that all the network traffic passes through it.

Since all the traffic passes through the SSG, it has all of the statistical information; however, it does not have Mobile IP session information. The Home Agent has the Mobile IP session information, and sends that information to the SSG.

The HA sends the following messages to the SSG/AAA server:

- Accounting Start: The HA sends this message to the SSG/AAA server when:
  - A MN successfully registers for the first time. This indicates the start of new Mobile IP session for a MN.
  - In case of redundant HA configuration, a stand-by HA will send an Accounting Start message only when it becomes active and it does not have any prior bindings. This allows the SSG to maintain host objects for MNs on failed HA. However, redundancy is not supported in Phase-1.
- Accounting Update: The HA generates an Accounting Update message if periodic accounting update message is configured, and when the mobile node changes its point of attachment (POA). For a Mobile IP session, this corresponds to a successful re-registration from a mobile node when it changes its care-of address (CoA). The CoA is the current location of the mobile node on the foreign network. Additionally, the HA sends an accounting update message with correct reject code when re-registration fails for an existing binding.
- Accounting Stop: The HA sends an Accounting Stop message when a RRP with error code is sent for an authenticated NAI (except for MobileIP error code 136), due and if binding does not exist for the NAI.

All the messages contain the following information:

- **Network Access Identifier (NAI)**: This is the MN's name. It looks similar to abc@service_provider1.com
- **Network Access Server (NAS) IP**: This is the accounting node's IP address. Since the HA is the accounting node, this field carries the HA address.
- **Framed IP Address**: This is the IP address of the MN. Typically the HA will allot an IP address to a MN after successful registration.
- **Point Of Attachment (POA)**: This field indicates the point of attachment for the MN on the network. For a mobile IP session, this is the MN's Care-Of-Address (COA).

## System Accounting in HA

An accounting-on is sent while a Home Agent is brought into the service (in other words, at the time of initialization after reloading a box), and if there is no active Home Agent at that time.

An accounting-off could be sent when the active Home Agent is taken out of service (graceful or otherwise), and if there is no standby Home Agent to provide the Home Agent service. Note that, accounting-off is not guaranteed.

An accounting-off is not sent when the standby Home Agent is taken out of service (graceful or otherwise).

## Messages Not Sent By Mobile IP Home Agent

The following messages are not sent by Mobile IP Home Agent.

- Accounting On Message (Acct-Status-Type=Accounting-On) when the HA box comes online or boots up: This message is a global entity for the platform, irrespective of Mobile IP configuration. This message is typically implemented by the platform code during initialization, and not by a service such as Mobile IP.
- Accounting Off Message (Acct-Status-Type=Accounting-Off) when the HA box is shutdown: This message is also a global entity for the platform, irrespective of Mobile IP configuration. This message is typically implemented by the platform code during reboot, and not by a service such as Mobile IP.

# Configuring HA Accounting

Mobile IP currently uses AAA commands to configure authorization parameters. All of the following commands are required. By default, the HA Accounting feature will be disabled; the HA will not send accounting messages to the AAA server unless configured. To enable the HA Accounting feature, perform the following tasks:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Router(config)# ip mobile home-agent accounting list` | Enables HA accounting, and applies the previously defined accounting method list for Home Agent. *list* is the AAA Accounting method used to generate HA accounting records. |
| **Step 2** | `Router(config)# ip mobile home-agent method redundancy [virtual-network address address] periodic-sync` | Syncs the byte and packet counts for each binding to the standby unit using an accounting update event. This sync only occurs if the byte counts have changed since the last sync. |
| **Step 3** | `Router(config)# aaa accounting network method list name start-stop group group name` | Sends a “start” accounting notice at the beginning of a process, and a “stop” accounting notice at the end of a process. The “start” accounting record is sent in the background. The requested user process begins regardless of whether the “start” accounting notice is received by the accounting server. |
| **Step 4** | `Router(config)# aaa accounting update newinfo` | Enables an interim accounting record to be sent to the accounting server whenever there is new accounting information to report relating to the user in question. |
| **Step 5** | `Router(config)# aaa accounting system default start-stop group radius` | Enables the HA to send system messages. |
| **Step 6** | `Router# debug aaa accounting` | Enables debugging of HA Accounting messages. |
| **Step 7** | `Router# debug radius`<br>`Router# debug tacacs` | Enables debugging of security protocol specific messages. |
| **Step 8** | `Router# debug ip mobile` | Enable Mobile IP related debug messages. Accounting will print debug messages only in case of errors. |

# HA Accounting Configuration Examples

The first block of commands are AAA configurations. An accounting method list (mylist) is created for network accounting. Start-Stop keywords imply that HA will send Start and Stop records. For detailed information, see the *IOS Security Configuration Guide*.

The Second line instructs the HA to send accounting Update records, whenever there is a change in Care-Of-Address (COA).

```
ip mobile home-agent accounting mylist address 10.3.3.1
ip mobile host 10.3.3.2 3.3.3.5 interface Ethernet2/2
ip mobile secure host 10.3.3.2 spi 1000 key ascii test algorithm md5 mode prefix-suffix
!
```

These are Mobile IP commands. On the first line, accounting method list mylist is applied on the Home Agent, thus enabling HA Accounting.

```
!
!
radius-server host 172.16.162.173 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
!
```

These are RADIUS commands. The first line specifies the RADIUS server address. Make sure the HA can reach the AAA server and has proper access privileges.

Here is a sample HA Accounting configuration:

**ACTIVE HA:**

```
router#
router#show run
Building configuration...

Current configuration : 4927 bytes
!
! Last configuration change at 05:12:03 UTC Thu Oct 13 2005
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname cisco7200
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa authentication ppp default local group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default local group radius
aaa authorization configuration default group radius
aaa accounting update newinfo periodic 2
aaa accounting network mylist start-stop group radius
aaa accounting system default start-stop group radius
!
```

```
!
aaa session-id common
!
resource manager
!
no ip subnet-zero
!
!
ip cef
no ip dhcp use vrf connected
ip dhcp ping packets 0
!
!
ip dhcp-server 99.107.0.13
vpdn-group 1
! Default L2TP VPDN group
! Default PPTP VPDN group
 accept-dialin
  protocol any
  virtual-template 1
!
!
no virtual-template snmp
!
!
username cisco7200 password 0 cisco
!
interface Loopback1
 ip address 11.0.0.1 255.0.0.0
!
interface FastEthernet0/0
 description "LINK TO HAAA.................!"
 ip address 150.2.13.40 255.255.0.0
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 duplex half
 no cdp enable
 standby 4 ip 150.2.0.252
 standby 4 priority 110
 standby 4 preempt delay reload 300
 standby 4 name cisco1
!
interface FastEthernet1/0
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface FastEthernet2/0
 description "LINK TO PDSN.................!"
 ip address 7.0.0.10 255.0.0.0
 no ip route-cache cef
 no ip route-cache
 duplex half
 standby 2 ip 7.0.0.2
 standby 2 priority 110
 standby 2 preempt delay reload 300
 standby 2 name cisco
!
interface FastEthernet3/0
```

```
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
 bridge-group 4
 bridge-group 4 spanning-disabled
!
interface Ethernet6/0
 description ""LINK TO REFLECTOR...."
 ip address 99.107.0.19 255.255.0.0
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 duplex half
 no cdp enable
 standby 3 ip 99.107.89.67
 standby 3 priority 110
 standby 3 preempt delay reload 300
 standby 3 name reflector
!
interface Ethernet6/1
 description "LINK TO TFTP....."
 ip address 1.7.130.10 255.255.0.0
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 duplex half
 no cdp enable
!
interface Ethernet6/2
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet6/3
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet6/4
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet6/5
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
```

```
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet6/6
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet6/7
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Virtual-Template1
 no ip address
!
router mobile
!
ip local pool LNS-Pool 8.3.0.1 8.3.0.100
ip local pool ispabc-pool 40.0.0.101 40.0.0.255
ip default-gateway 10.1.2.13
ip classless
ip route 8.0.0.1 255.255.255.255 7.0.0.1
ip route 9.0.0.1 255.255.255.255 7.0.0.1
ip mobile home-agent accounting mylist broadcast
ip mobile home-agent redundancy cisco virtual-network address 7.0.0.2 periodic-sync
ip mobile virtual-network 40.0.0.0 255.0.0.0
ip mobile host nai @ispxyz.com address pool local ispabc-pool virtual-network 40.0.0.0
255.0.0.0 aaa lifetime 250
ip mobile secure home-agent 7.0.0.2 spi 1001 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 7.0.0.67 spi 1001 key ascii cisco algorithm md5 mode
prefix-suffix
!
no ip http server
!
!
ip radius source-interface Loopback1
access-list 120 deny   ip 40.0.0.0 0.255.255.255 40.0.0.0 0.255.255.255
access-list 120 permit ip any any
dialer-list 1 protocol ip permit
!
!
radius-server host 150.2.0.2 auth-port 1645 acct-port 1646
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send accounting 3gpp2
radius-server vsa send authentication 3gpp2
!
control-plane
!
dial-peer cor custom
!
!
gatekeeper
```

```
 shutdown
!
alias exec shb sh ip mob bin
alias exec shr sh ip route
alias exec sht sh ip mob tun
alias exec shh sh ip mob host
alias exec clr clear ip mob bin all
!
line con 0
 exec-timeout 0 0
 length 0
 stopbits 1
line aux 0
 exec-timeout 0 0
 password 7 0507070D
 length 0
 stopbits 1
line vty 0 4
 password 7 0507070D
!
no scheduler max-task-time
ntp master 1
ntp update-calendar
ntp server 30.1.0.1
!
end

router#
```

**STANDBY HA:**

```
router#
router#show run
Building configuration...

Current configuration : 3995 bytes
!
! No configuration change since last restart
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname cisco7200
!
boot-start-marker
boot system tftp /auto/tftpboot-users/tennis/c7200-h1is-mz.123-3.8.PI2 171.69.1.129
boot-end-marker
!
enable password 7 00445566
!
no spd enable
aaa new-model
!
!
aaa authentication ppp default local group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default local group radius
```

```
aaa authorization configuration default group radius
aaa accounting update newinfo periodic 2
aaa accounting network mylist start-stop group radius
aaa accounting system default start-stop group radius
!
!
aaa session-id common
!
resource manager
!
ip subnet-zero
!
!
no ip cef
ip ftp username pdsn-team
ip ftp password 7 pdsneng
ip host PAGENT-SECURITY-V3 32.68.10.4 38.90.0.0
ip name-server 11.69.2.133
no ip dhcp use vrf connected
!
!
vpdn enable
vpdn ip udp ignore checksum
!
vpdn-group 1
! Default L2TP VPDN group
! Default PPTP VPDN group
 accept-dialin
  protocol any
  virtual-template 1
!
!
no virtual-template snmp
!
username mwt13-7200b password 0 cisco
!
interface Loopback1
 ip address 11.0.0.1 255.0.0.0
 no ip route-cache
!
interface FastEthernet0/0
 ip address 4.0.10.2 255.0.0.0
 no ip route-cache
 duplex half
 no cdp enable
!
interface FastEthernet1/0
 no ip address
 no ip route-cache
 duplex half
 no cdp enable
!
interface FastEthernet2/0
 description "LINK TO HAAA.............!"
 ip address 15.2.13.20 255.255.0.0
 no ip route-cache
 duplex full
 no cdp enable
 standby 4 ip 15.2.0.252
 standby 4 name cisco1
!
interface FastEthernet5/0
 description "LINK TO PDSN.............!"
 ip address 7.0.0.67 255.0.0.0
```

```
 no ip route-cache
 duplex full
 standby 2 ip 7.0.0.2
 standby 2 name cisco
!
interface Ethernet6/0
 description "LINK TO REFLECTOR....!"
 ip address 22.107.0.12 255.255.0.0
 no ip route-cache
 no ip mroute-cache
 duplex half
 no cdp enable
 standby 3 ip 22.107.89.67
 standby 3 name reflector
!
interface Ethernet6/1
 description "LINK TO TFTP....."
 ip address 1.7.130.2 255.255.0.0
 no ip route-cache
 duplex half
 no cdp enable
!
interface Ethernet6/2
 no ip address
 no ip route-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet6/3
 no ip address
 no ip route-cache
 shutdown
 duplex half
 no cdp enable
!
router mobile
!
ip local pool LNS-Pool 8.3.0.1 8.3.0.100
ip local pool ispabc-pool 40.0.0.101 40.0.0.255
ip default-gateway 10.1.2.13
ip classless
ip route 8.0.0.1 255.255.255.255 7.0.0.1
ip route 9.0.0.1 255.255.255.255 7.0.0.1
ip mobile home-agent accounting mylist broadcast
ip mobile home-agent redundancy cisco virtual-network address 7.0.0.2 periodic-sync
ip mobile virtual-network 40.0.0.0 255.0.0.0
ip mobile host nai @ispxyz.com address pool local ispabc-pool virtual-network 40.0.0.0
255.0.0.0 aaa lifetime 250
ip mobile secure home-agent 7.0.0.2 spi 1001 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 7.0.0.10 spi 1001 key ascii cisco algorithm md5 mode
prefix-suffix
!
no ip http server
!
!
ip radius source-interface Loopback1
dialer-list 1 protocol ip permit
!
!
radius-server host 150.2.0.2 auth-port 1645 acct-port 1646
radius-server key cisco
radius-server vsa send accounting
```

```
radius-server vsa send accounting 3gpp2
radius-server vsa send authentication 3gpp2
!
control-plane

!
gatekeeper
 shutdown
!
alias exec shb sh ip mob bin
alias exec shr sh ip route
alias exec sht sh ip mob tun
alias exec shh sh ip mob host
alias exec clr clear ip mob bin all
!
line con 0
 exec-timeout 0 0
 length 0
 stopbits 1
line aux 0
 exec-timeout 0 0
 length 0
 stopbits 1
line vty 0 4
 password 7 0507070D
!
no scheduler max-task-time
ntp master 1
ntp update-calendar
ntp server 30.1.0.1
!
end
```

## Verifying HA Accounting Setup

The HA Accounting status can be verified by issuing the **show ip mobile global** command. The current accounting status is displayed as shown below:

```
router# sh ip mobile global
IP Mobility global information:

Home Agent

    Registration lifetime: 10:00:00 (36000 secs)
    Broadcast enabled
    Replay protection time: 7 secs
    Reverse tunnel enabled
    ICMP Unreachable enabled
    Strip realm disabled
    NAT Traversal disabled
    HA Accounting enabled using method list: mylist
    NAT UDP Tunneling support enabled
    UDP Tunnel Keepalive 110
    Forced UDP Tunneling disabled
    Standby groups
        cisco (virtual network - address 7.0.0.2)
    Virtual networks
        40.0.0.0 /8
```

```
Foreign Agent is not enabled, no care-of address

0 interfaces providing service
Encapsulations supported: IPIP and GRE
Tunnel fast switching enabled, cef switching enabled
Tunnel path MTU discovery aged out after 10 min
Radius Disconnect Capability disabled
```

router#

CHAPTER 1

# Multi-VPN Routing and Forwarding on the Home Agent

This chapter discusses the functional elements of the Multi-VPN Routing and Forwarding (VRF) CE network architecture, and their implementation in Cisco IOS Mobile Wireless Home Agent software.

This chapter includes the following sections:



## VRF Support on HA

The HA supports overlapping IP addresses for mobile nodes for the mobile IP flows that are opened for different realms. This feature is based on the Multi-VPN Routing and Forwarding (VRF) Customer Edge (CE) network architecture, and expands the BGP/MPLS VPN architecture to support multiple VPNs (and therefore multiple customers) per CE device. This reduces the amount of equipment required, and simplifies administration, and allows the use of overlapping IP address spaces within the CE network.

Multi-VRF CE is a new feature, introduced in Cisco IOS release 12.2(4)T, that addresses these issues. Multi-VRF CE, also known as VRF-Lite, extends limited PE functionality to a Customer Edge (CE) router in an MPLS-VPN model. A CE router now has the ability to maintain separate VRF tables in order to extend the privacy and security of an MPLS-VPN down to a branch office rather than just at the PE router node. The CE can support traffic separation between customer networks, or between entities within a single customer network. Each VRF on the CE router is mapped to a corresponding VRF on the PE router.

For more information on Multi-VRF CE network architecture, please refer to Cisco Product Bulletin 1575 at the following URL: http://www.cisco.com/warp/public/cc/pd/rt/2600/prodlit/1575_pp.pdf.

*Figure 1-1 VRF-Lite in the Cisco PDSN/Home Agent Architecture*

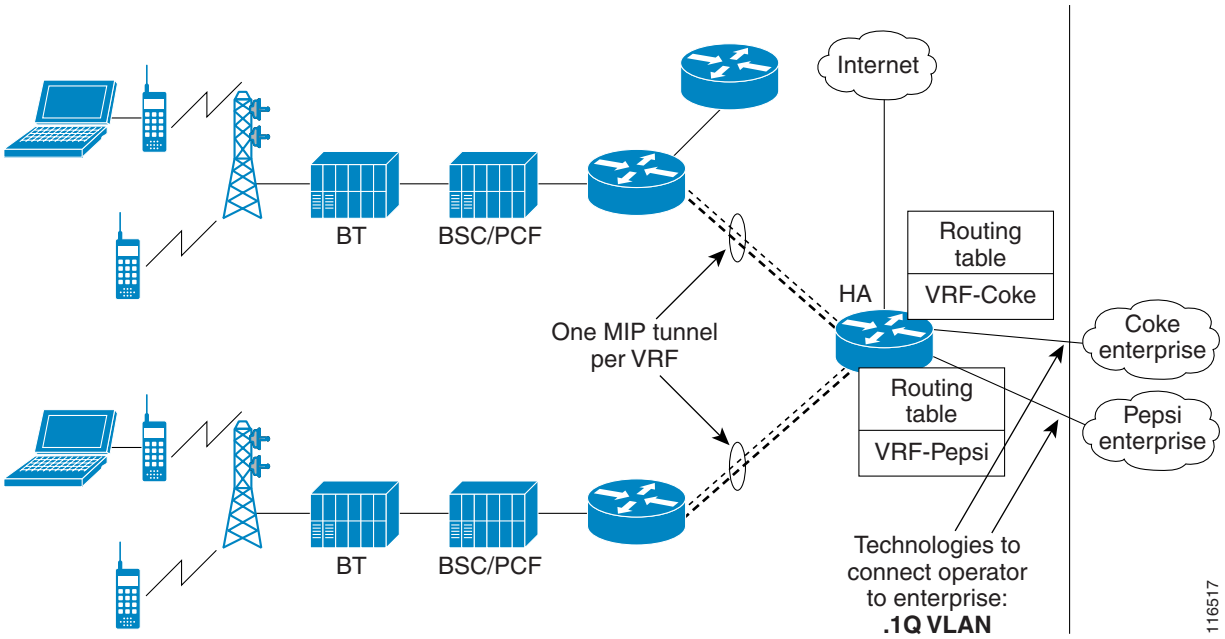



Figure 1-1 illustrates the PDSN architecture and how the VRF-lite solution is applied to the Home Agent for different realms and enterprises, thus segregating data between the enterprises.

Highlights of the VRF solution include the following:

- Provides a method to identify the VRF of the user that is based on domain or realm of the user.
- Provides a method to ensure delivery of packets to the mobile (through the PDSN) when different mobiles belonging to different enterprises share the same overlapping IP address.
- Supports IP address and routing table management per VRF.
- Supports management of VRF per enterprise/domain.
- Supports AAA authentication and accounting group per VRF.

The realm is used to identify an enterprise network. One virtual Home Agent is configured per realm. NAI is part of Mobile IP RRQ, and is the main identifier of mobile IP users in the PDSN and HA. The realm part of NAI will be used to identify the virtual Home Agent. Mobile nodes follow the NAI convention of *username@company*, where *company* identifies a realm name that indicates a subscriber community.

Multiple IP addresses are used at the HA to indicate different enterprise connections or VRFs to the PDSN. Thus, there will be one mobile IP tunnel between the PDSN and the HA per realm/VRF.

For an HA that is connected to two enterprises, “abc.com” and “xyz.com,” the HA will be configured with two unique IP addresses (typically configured under a loopback interface). The PDSN will have a MoIP tunnel to an address LA1 to reach “abc.com,” and will have another MoIP tunnel to address LA2 to reach “xyz.com,” where LA1 and LA2 are IP addresses configured under a Loopback interface.

On the home AAA RADIUS server, the NAI/domain configuration ensures that the PDSN receives LA1 as the IP address of the Home Agent of enterprise “xyz.com” as part of the Access Response during FA-CHAP or HA-CHAP (MN-AAA authentication); and LA2 as the IP address of Home Agent of enterprise “mnp.com”.

This feature will work with HA-SLB solution for HA load balancing.

## Mobile IP Tunnel Establishment

The following procedure describes a mobile IP flow establishment with HA-SLB and VRF enabled. Elements in this call flow are two Mobile nodes (MN-1 and MN-2) belonging to enterprise ENT-1 & ENT-2 respectively:

**Step 1** When a Mobile IP RRQ arrives at the HA, the HA reads the NAI field of the incoming RRQ, and selects a pre-configured IP address to form a Mobile IP tunnel back to the PDSN using this IP address as the source address of the tunnel.

**Step 2** The "Home-Agent address" field in the RRP that is being sent to the PDSN is modified to the IP address as described above.

**Step 3** The Home Agent adds a host route that corresponds to the IP address assigned to the mobile in the routing table that corresponds to the VRF defined for the realm.

**Step 4** The tunnel end-point at the HA is also inserted in the VRF routing table. This enables the mobiles to share common IP address across different realms on the same Home Agent.

**Step 5** MN-1 sends a Mobile IP RRQ with Home Agent address set to 0.0.0.0 (dynamic Home Agent) to the PDSN over its R-P session.

**Step 6** The PDSN initiates FA-CHAP and sends an Access Request to AAA.

**Step 7** AAA responds with an Access Response, the Home Agent address returned is the IP address of HA-SLB.

**Step 8** The PDSN forwards a MIP RRQ to the HA-SLB.

**Step 9** The HA-SLB determines the real HA based on load, and forwards the RRQ to HA1.

**Step 10** HA-1 receives the MIP RRQ. It parses the NAI inside the message and determines the VRF of the user based on its realm - enterprise Ent-1. It performs HA-CHAP (MN-AAA authentication), allocates an IP address to the mobile for Ent-1. It creates a binding for the mobile and populates VRF specific data structures (like route entry in route-table of VRF, FIB, etc.).

**Step 11** HA1 sends a MIP RRP to the PDSN, and also establishes a mobile IP tunnel between the PDSN and the HA. The end point of the tunnel on the HA is L1-IP-1 (rather than the IP address of the ingress interface in the MIP RRQ).

## VRF Mapping on the RADIUS Server

In this release, the VRF feature is enhanced to configure the NAI to VRF mapping on the RADIUS server. Mobile to VRF mapping occurs as follows with this enhancement.

1. When a mobileip registration request is received, the HA sends a radius access request.
2. The AAA server sends access accept with VRF name, in radius attribute “cisco-avpair = mobileip:ip-vrf”, and the corresponding home-agent address in RADIUS attribute “cisco-avpair = mobileip-vrf-ha-addr” to the HA.
3. The Home Agent uses this information to open the binding and associates it with the correct VRF. If the above attributes are not downloaded from AAA server, then the locally configured VRF, if any, is used.
4. Additionally, an option is provided to send a registration reply with code 136 and a new home agent address, if the HA has to assign a different address than requested by the PDSN/FA.
5. Upon receiving a registration reply with code 136, the mobile sends one more registration request with a new address.
6. The HA processes the request, opens a binding, and sends a registration reply (success) thus completing the registration process

## VRF Feature Restrictions

The following list identifies restrictions for the VRF feature:

- Only static IP routing between the Home Agent and the CE devices is supported. Dynamic routing protocols (for example, OSPF) are not supported to redistribute mobile routes that are added in Home Agent.
- A maximum of 200 VRFs per Home Agent is supported.

The Home Agent MIB is not updated with the VRF information.

## Authentication and Accounting Server Groups Per Realm

Separate authentication and accounting groups can be specified across different realms. Based on the realm of the user, the HA will choose the AAA authentication server based on the authentication group specified for the realm on the HA. Similarly, the HA will choose a AAA accounting server based on the realm of the user if the accounting group is specified for the realm.

**Note** This feature will work in conjunction with the VRF feature.

## Configuring VRF for the HA

To configure VRF on the HA, perform the following tasks:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Router(config)#ip mobile realm` *@xyz.com* `vrf` *vrf-name* `ha-addr` *ip-address* [`aaa-group` [`accounting` *aaa-acct-group* \| `authentication` *aaa-auth-group*]] | Defines the VRF for the domain *@xyz.com*.<br>The IP address of the Home Agent that corresponds to the VRF is also defined at the point that the MOIP tunnel will terminate.<br>The IP address of the Home Agent should be a routable IP address on the box.<br>Optionally, the AAA accounting and/or authentication server groups can be defined per VRF.<br>If AAA accounting server group is defined, all accounting records for the users of the realm will be sent to the specified group.<br>If AAA authentication server group is defined, HA-CHAP (MN-AAA authentication) is sent to the server(s) defined in the group. |
| **Step 2** | `Router(config)# ip vrf` *vrf-name*<br>`description VRF for domain1`<br>`rd 10:1` | Defines the VRF on the box.<br>Description of the VRF.<br>Router descriptor for VRF. Creates a VRF table by specifying a route distinguisher.<br>**Note** One VRF per domain should be configured on each HA CPU. |
| **Step 3** | `router# interface Loopback1`<br>`ip address 192.168.11.1 255.255.255.0 secondary`<br>`ip address 192.168.10.1 255.255.255.0` | Defines the loopback interface under which the IP addresses for each VRF are configured. These addresses are used as the Mobile IP tunnel source IP addresses for the realm.<br>The mask that is configured for the IP address will be used in the VRF routing table. Host mask (255.255.255.255) or broadcast mask (0.0.0.0) should not be configured. |

Here is an example of how to configure the User profile for VRF:

```
[ //localhost/Radius/Profiles/mwts-mip-r20sit-haslb1-prof/Attributes ]
    CDMA-HA-IP-Addr = 20.20.225.1
    CDMA-MN-HA-Shared-Key = ciscociscociscoc
    CDMA-MN-HA-SPI = 00:00:10:01
    CDMA-Reverse-Tunnel-Spec = "Reverse tunneling is required"
    cisco-avpair = mobileip-vrf-ha-addr=20.20.204.2
    cisco-avpair = ip:ip-vrf#0=ispxyz-vrf1
    class = "Entering the World of Mobile IP-3"
```

Service-Type = Framed

# VRF Configuration Example

The following is a sample configuration on an MWAM HA with VRF support:

```
CiscoHA#show running-config
Building configuration...

Current configuration : 3366 bytes
!
...
!
aaa new-model
!
!
aaa group server radius vrf-auth-grp1
 server 9.15.100.1 auth-port 1645 acct-port 1646
!
aaa group server radius vrf-auth-grp2
 server 10.76.86.8 auth-port 1645 acct-port 1646
!
aaa authentication ppp vrf-auth-grp1 group vrf-auth-grp1
aaa authentication ppp vrf-auth-grp2 group vrf-auth-grp2
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network vrf-auth-grp1 group vrf-auth-grp1
aaa authorization network vrf-auth-grp2 group vrf-auth-grp2
aaa authorization configuration default group radius
aaa accounting network default start-stop group radius
aaa accounting network vrf-auth-grp1 start-stop group vrf-auth-grp1
aaa accounting network vrf-auth-grp2 start-stop group vrf-auth-grp2
aaa session-id common
ip subnet-zero
no ip gratuitous-arps
ip cef
no ip domain lookup
!
!
ip vrf moip-vrf-grp1
 rd 100:1
!
ip vrf moip-vrf-grp2
 rd 100:2
!
no virtual-template snmp
!
!
!
interface Loopback1
 ip address 172.16.11.1 255.255.255.0 secondary
 ip address 172.16.10.1 255.255.255.0
!
interface GigabitEthernet0/0
 no ip address
!
interface GigabitEthernet0/0.11
 encapsulation dot1Q 11
 ip address 9.15.42.111 255.255.0.0
 no cdp enable
!
interface GigabitEthernet0/0.82
 description Interface towards PDSN
 encapsulation dot1Q 82
 ip address 10.82.82.2 255.255.0.0
```

```
!
router mobile
!
ip local pool vrf-pool1 10.5.5.1 5.5.5.254 group vrf-pool-grp1
ip local pool vrf-pool2 10.5.5.1 5.5.5.254 group vrf-pool-grp2
ip classless
ip route 10.15.47.80 255.255.255.255 GigabitEthernet0/1
ip route 10.76.86.8 255.255.255.255 9.15.0.1
ip route 10.1.0.0 255.255.0.0 GigabitEthernet0/0.82
no ip http server
!
ip mobile home-agent
ip mobile host nai @xyz.com address pool local vrf-pool2 interface GigabitEthernet0/0.82
aaa
ip mobile host nai @cisco.com address pool local vrf-pool1 interface GigabitEthernet0/0.82
aaa
ip mobile realm @xyz.com vrf moip-vrf-grp2 ha 172.16.11.1 aaa-group accounting
vrf-auth-grp1 authentication vrf-auth-grp2
ip mobile realm @cisco.com vrf moip-vrf-grp1 ha 172.16.10.1 aaa-group accounting
vrf-auth-grp2 authentication vrf-auth-grp1
!
!
!
radius-server host 10.15.100.1 auth-port 1645 acct-port 1646 key cisco
radius-server host 10.76.86.8 auth-port 1645 acct-port 1646 key cisco
!
control-plane
!
...
!
end
```

# VRF Configuration with HA Redundancy Example

The following is a sample configuration on a Cisco 7200 HA with HA redundancy and VRF. The following steps are required:

**Step 1** Configure normal HSRP and HA redundancy for the published HA IP address.

**Step 2** Rather than configuring IP addresses on the Loopback (or any other interface IP addresses for tunnel end-point), configure them on the HSRP interface as a secondary standby IP address.

**Step 3** For IP mobile redundancy, add virtual network for VRF tunnel point subnet.

**Step 4** Configure the VRF related commands.

**Step 5** Because the binding update message from active to the standby HA contains the NAI, the standby is able to create the binding using appropriate VRF using the domain of the NAI in the message.

```
Active HA:
HA1#sh run
...
aaa new-model
!
!
aaa group server radius vrf-auth-grp1
 server 9.15.100.1 auth-port 1645 acct-port 1646
!
```

```
aaa group server radius vrf-auth-grp2
 server 10.76.86.8 auth-port 1645 acct-port 1646
!
aaa authentication ppp default local group radius
aaa authentication ppp vrf-auth-grp1 group vrf-auth-grp1
aaa authentication ppp vrf-auth-grp2 group vrf-auth-grp2
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa authorization network vrf-auth-grp1 group vrf-auth-grp1
aaa authorization network vrf-auth-grp2 group vrf-auth-grp2
aaa authorization configuration default group radius
aaa session-id common
ip subnet-zero
ip gratuitous-arps
!
!
ip cef
no ip domain lookup
!
!
ip vrf moip-vrf
 rd 100:1
!
ip vrf moip-vrf1
 rd 100:2
!
...
!
interface FastEthernet1/0
 ip address 10.92.92.2 255.255.0.0
 duplex auto
 speed auto
 no cdp enable
 standby 10 ip 10.92.92.12
 standby 10 ip 172.16.11.1 secondary
 standby 10 ip 172.16.12.1 secondary
 standby 10 priority 130
 standby 10 preempt delay sync 10
 standby 10 name cisco
!
!
router mobile
!
ip local pool vrf-pool1 10.5.5.5 5.5.5.55 group vrf-pool-grp1
ip local pool vrf-pool2 10.5.5.5 5.5.5.55 group vrf-pool-grp2
ip classless
ip mobile home-agent address 10.92.92.12
ip mobile home-agent redundancy cisco virtual-network address 192.168.0.0
ip mobile host nai @cisco.com address pool local vrf-pool1 interface FastEthernet1/0 aaa
ip mobile host nai @xyz.com address pool local vrf-pool2 interface FastEthernet1/0 aaa
ip mobile realm @cisco.com vrf moip-vrf home-agent-address 192.168.11.1 aaa-group
authentication vrf-auth-grp1
ip mobile realm @xyz.com vrf moip-vrf1 home-agent-address 192.168.12.1 aaa-group
authentication vrf-auth-grp2
ip mobile secure home-agent 10.92.92.3 spi 101 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 172.16.11.1 spi 101 key ascii cisco algorithm md5 mode
prefix-suffix
...
radius-server host 10.76.86.8 auth-port 1645 acct-port 1646 key cisco
radius-server host 10.15.100.1 auth-port 1645 acct-port 1646 key cisco
!
...
```

```
end

Standby HA:
HA2#sh run
...
!
aaa new-model
!
aaa group server radius vrf-auth-grp1
 server 10.15.100.1 auth-port 1645 acct-port 1646
!
aaa group server radius vrf-auth-grp2
 server 10.76.86.8 auth-port 1645 acct-port 1646
!
aaa authentication ppp default group radius
aaa authentication ppp vrf-auth-grp1 group vrf-auth-grp1
aaa authentication ppp vrf-auth-grp2 group vrf-auth-grp2
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa authorization network vrf-auth-grp1 group vrf-auth-grp1
aaa authorization network vrf-auth-grp2 group vrf-auth-grp2
aaa session-id common
ip subnet-zero
!
!
ip cef
!
!
ip vrf moip-vrf
 rd 100:1
!
ip vrf moip-vrf1
 rd 100:2
!
...
!
interface FastEthernet1/0
 ip address 10.92.92.3 255.255.255.0
 duplex auto
 speed auto
 standby 10 ip 10.92.92.12
 standby 10 ip 172.16.11.1 secondary
 standby 10 ip 172.16.12.1 secondary
 standby 10 preempt delay sync 10
 standby 10 name cisco
!
...
!
router mobile
!
ip local pool vrf-pool1 10.5.5.5 5.5.5.55 group vrf-pool-grp1
ip local pool vrf-pool2 10.5.5.5 5.5.5.55 group vrf-pool-grp2
ip mobile home-agent address 10.92.92.12
ip mobile home-agent redundancy cisco virtual-network address 192.168.0.0
ip mobile host nai @cisco.com address pool local vrf-pool1 interface FastEthernet1/0 aaa
ip mobile host nai @xyz.com address pool local vrf-pool2 interface FastEthernet1/0 aaa
ip mobile realm @cisco.com vrf moip-vrf home-agent-address 192.168.11.1 aaa-group
authentication vrf-auth-grp1
ip mobile realm @xyz.com vrf moip-vrf1 home-agent-address 192.168.12.1 aaa-group
authentication vrf-auth-grp2
ip mobile secure home-agent 10.92.92.2 spi 101 key ascii cisco algorithm md5 mode
prefix-suffix
```

```
ip mobile secure home-agent 172.16.11.1 spi 101 key ascii cisco algorithm md5 mode
prefix-suffix ignore-spi
ip mobile secure home-agent 172.16.12.1 spi 101 key ascii cisco algorithm md5 mode
prefix-suffix
no ip http server
!
...
radius-server host 10.76.86.8 auth-port 1645 acct-port 1646 key cisco
radius-server host 10.15.100.1 auth-port 1645 acct-port 1646 key cisco
...
end
```

CHAPTER 1

# Monitoring Upstream User Traffic

This chapter discusses how to monitor upstream user traffic using the Hotlining feature, and provides details on how to configure the feature on the Cisco Mobile Wireless Home Agent.

This chapter includes the following sections:



## Hot-lining

The Cisco Mobile Wireless Home Agent supports hot-lining for mobile nodes based on the Nortel X31-20031013-0xx (October 2003). The hot-lining feature enables you to monitor upstream user traffic using two different scenarios—active and new session. When hot-lining is active for a particular user, the upstream IP packets from the mobile are re-directed to the re-direct server that is configured for this particular realm. Re-direction is achieved by changing the IP packet destination address to the Re-direct server address. The only mandatory attribute supported in the Change of Authorization (CoA) message from the Home AAA server (HAAA)is the User-Name attribute to identify the particular user on the Home Agent. Optionally, the IP address can also be sent in the CoA message to identify the particular binding for a particular user.

### Active Session Hot-Lining

For active session hot-lining, the user starts a packet data session. In the middle of the session it is hot-lined and, after the account is reconciled, hot-lining on the session is removed. Hot-lining is done with a RADIUS Change of Authorization (CoA) message. The following procedure lists the events for active session Hot-lining:

**Step 1** Action for normal hot line profile is locally configured on the HA.

**Step 2** Action for active hot line profile is locally configured on the HA.

**Step 3** User joeusr@carrier.com is created at the Home AAA and assigned a normal hot line profile.

**Step 4** User joeusr@carrier.com registers with the HA.

**Step 5** The HA sends an Access Request to the HAAA for the user.

**Step 6** The HAAA responds with an Access Accept that contains a Filter-ID attribute set to normal.

**Step 7** The HA applies normal hot line action (no redirection) for the user.

**Step 8** The HA completes MIP registration by sending an RRP.

**Step 9** Some event occurs at this point to cause the user to be hot lined. The user hot line profile at the HAAA is modified to active.

**Step 10** The HAAA sends a Change of Authorization command with Filter-ID attribute set to active.

**Step 11** The RADIUS client at the HA ACKs the Change of Authorization command.

**Step 12** The HA applies active hot line action (redirection) for the user.

**Step 13** At this point, the user has taken action to reconcile the event that resulted in hot lining of the account. The hot line profile at the HAAA is modified to normal.

**Step 14** The HAAA sends a Change of Authorization command with Filter-ID attribute set to normal.

**Step 15** The RADIUS client at the HA ACKs the Change of Authorization command.

**Step 16** The HA applies normal hot line action (no redirection) for the user.

## New Session Hot-Lining

For new Session hot-lining, the user's session is hot-lined at the time of packet data session establishment. In this scenario the RADIUS Access-Accept message is used to hot-line the session. The following procedure lists the events for new session hot-lining:

**Step 1** Action for normal hot line profile is locally configured on the HA.

**Step 2** Action for active hot line profile is locally configured on the HA.

**Step 3** User joeusr@carrier.com is created at the HAAA and assigned an active hot line profile.

**Step 4** User joeusr@carrier.com registers with the HA.

**Step 5** The RADIUS client sends an Access Request for the user.

**Step 6** The Access Accept contains the Filter-ID attribute set to active.

**Step 7** The HA applies active hot line action (redirection) for the user.

## Restrictions for Hot-lining

The following list identifies restrictions for the hot-lining feature:

- The hot-lining feature supports only upstream IP packet level re-direction and downstream packets are not hot-lined. Firewall hot-lining is not supported.
- The Home Agent does not support Correlation ID and NAS-Identifier attributes in the CoA request received from AAA.
- Hot lining is not supported with HA redundancy.
- On the Home Agent, the hot-lining policy is applied only when the policy is downloaded during HA CHAP.

- The Home Agent will not reject the RRQ if reverse-tunnel is not requested by the user and hot lining policy is downloaded for the user.
- The Home Agent will not notify packet data users the reason for their hot-lined status prior to denial of data service.
- The Home Agent MIB is not updated with the hot-lining information.

## Configuring Hot-Lining

To configure Hot-lining, perform the following tasks in global configuration mode:

| Command | Purpose |
|---|---|
| `Router(config)# ip mobile realm` *realm* `hotline redirect` *redirect-server-ipaddress* | Enables inbound user sessions to be disconnected when specific session attributes are presented. |
| `Router(config)# ip mobile cdma-ipsec fa-address` *ip address* `security-level` *1\|2* | Sets the security level with the PDSN specified by the *ip address*. |

CHAPTER 1

# Other Configuration Tasks


# Other Configuration Tasks


This chapter discusses important concepts and provides configuration details for the following features in the Cisco IOS Mobile Wireless Home Agent software:



## Support for ACLs on Tunnel Interface

The Cisco Tunnel Templates feature allows the configuration of ACLs on statically created tunnels to be applied to dynamic tunnels brought up on the Home Agent. A tunnel template is defined and applied to the tunnels between the Home Agent and PDSN/Foreign Agent.

## Configuring Mobile IP Tunnel Template Feature

To enable the Mobile IP Tunnel Template feature, perform these tasks:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Router(config)# interface tunnel 10`<br>`ip access-group 150` | Configures an interface type and enters interface configuration mode.<br>**tunnel** interface; a virtual interface. The number is the number of the tunnel interface that you want to create or configure. There is no limit on the number of tunnel interfaces that you can create. |
| **Step 1** | `Router(config)# access-list 150 deny any  10.10.0.0 0.255.255.255`<br>`access-list permit any any` | Configures the access list mechanism for filtering frames by protocol type or vendor code |
| **Step 1** | `Router(config)# ip mobile home-agent template tunnel 10 address 10.0.0.1` | Configures the template tunnel and the template tunnel address. |

Here is a sample configuration used to block certain traffic using template tunnel feature:

1. Configure a tunnel template

```
interface tunnel 10
     ip access-group 150 in -------> apply access-list 150
```

2. Configure the ACL

```
access-list 150 deny any  10.10.0.0 0.255.255.255
access-list permit any any
          ------> permit all but traffic to 10.10.0.0 network
```

3. Configure the Home Agent to use the template tunnel.

```
ip mobile home-agent template tunnel 10 address 10.0.0.1
```

**Note** If you enable the Mobile IP Tunnel Template feature and remove the tunnel interface from the configuration, you should also manually remove the corresponding **mobileip tunnel template** command. If necessary, you can reconfigure the **mobileip tunnel template** command after you configure a new tunnel interface.

### Limitations

When you use PMIP with session redundancy and you choose the "msec" option for the timestamp (**ip mobile foreign-service revocation timeout** 5 **retransmit** 4 **timestamp msec**), and open a PMIP flow with PDSN SR setup, the **cdma redundancy debug** output shows that the "revocation timestamp" value on the active and standby PDSNs are the same.

If you perform a switchover, the standby PDSN takes over as active. If you try to close the PMIP flow, the revocation message sent from the PDSN to the HA is ignored on HA because the timestamp is mismatched. Thus, after several re-tries, the PDSN deletes the revocation entry pending for Ack, and the binding on the HA is not deleted.

This limitation is not related to synching the attribute, but to the uptime of the router, because the **msec** option puts the uptime in the timestamp field and the uptime of the standby router is expected to be lower. If you utilize the default **seconds** based option (which puts a timestamp in UTC), this may not be an issue. Additionally, **msec** has another issue of wrap-around in 49+ days, so it cannot be used in an always-on setup.

# Support for AAA Attributes MN-HA-SPI and MN-HA SHARED KEY

The Cisco Home Agent supports the following 3GPP2 standard attributes:

MN-HA-SPI (26/57)

MN-HA-SHARED-KEY (26/58)

The following procedure illustrates this support:

**Step 1** The HA receives a RRQ from the PDSN/FA

**Step 2** The HA sends an Access Request to AAA. The HA adds the MHAE SPI of the RRQ to the Access Request as MN-HA-SPI(26/57) attribute.

**Step 3** The AAA server matches the MN-HA-SPI (26/57) against the corresponding MN-HA-SHARED-KEY (26/58).

**Step 4** The AAA server includes that MN-HA-SHARED-KEY (26/58) in the access reply.

**Step 5** The HA authenticates the MHAE of RRQ using the downloaded shared key MN-HA-SHARED-KEY (26/58).

# User Profiles

The Home Agent maintains a per NAI profile that contains the following parameters:

- User Identification - NAI
- User Identification - IP Address
- Security Associations
- Reverse Tunnel indication - the parameter specifies the style of reverse tunneling that is required for the user data transfer with Mobile IP services.
- Timestamp window for replay protection
- State information is maintained for all Registration Request flags requested, and then granted (for example, S|B|D|M|G|V flags).

  The profile, identified by the NAI, can be configured locally or retrieved from a AAA server.

Additionally, the Home Agent supports an intelligent security association caching mechanism that optimizes the session establishment rate and minimizes the time for session establishment.

The Home Agent supports the local configuration of a maximum of 200000 user profiles; on the MWAM, the HA supports 5 x 200000 user profiles. The User profile, identified by the NAI, can be configured locally, or retrieved from a AAA server.

# Mobility Binding Association

The mobility binding is identified in the Home Agent in the following ways:

- For static IP address assignment, NAI+IP
- For dynamic IP address assignment, NAI
- The **show ip mobile binding** command will show mobility binding information for each user.

The binding association contains the following information:

- Care-of-Address
- Home address
- Lifetime of the association
- Signalling identification field

# HA Binding Update

When a mobile first registers for packet data services, a PPP session and associated Mobile IP flow(s) are established at the PDSN. In the event of an inter-PDSN handoff, another PPP session is established at the target PDSN, and the mobile registers with the Home Agent using the new PDSN/FA. If PPP idle-timeout is configured on the PDSN virtual-template, the maximum mobile IP lifetime advertised to the mobile will be 1 second less than the idle-timeout.

Idle, or unused PPP sessions at a PDSN/Foreign Agent consume valuable resources. The Cisco PDSN/Foreign Agent and Home Agent support Binding Update and Binding Acknowledge messages to release such idle PPP sessions as soon as possible. In the event of an inter-PDSN handoff and Mobile IP registration, the Home Agent updates mobility binding information for the mobile with the Care-of-Address (CoA) of the new PDSN/FA.

If simultaneous bindings are not enabled, the Home Agent sends a notification in the form of a Binding Update message to the previous PDSN/FA. The previous PDSN/FA acknowledges with a Binding Acknowledge, if required, and deletes the visitor list entry for the Mobile IP session. The previous PDSN/FA initiates the release of the PPP session when there are no active flows for that mobile station.

**Note** You can configure the Home Agent to send the binding update message on a global basis.

**Note** This feature works with a Cisco FA that has bind update enabled on the box. Security association between the FA and HA has to be configured on both the boxes for this feature to be enabled.

# Selective Mobile Blocking

You might want to block access to a specific mobile for reasons such as prepaid quota is over, service is disabled due to non-payment of bills, or other reasons. You can accomplish this by adding the "mobileip:prohibited" cisco-avpair attribute to the user profile on AAA server. When the "mobileip:prohibited" attribute is returned to Home Agent in access accept, the behavior is as follows:

- If the AAA server returns "mobileip:prohibited=1" in an access accept, and if the MN-HA Security Association for the mobile is configured on the AAA server and also returned to Home Agent in an access accept, the Home Agent sends a registration request (failure) with error code 129 (Administratively Prohibited) to the MN.
- If the AAA server returns "mobileip:prohibited=0" in an access accept, or if the attribute is not returned to the HA in an access accept, the HA performs normal processing of the registration request.

**Note** The "mobileip:prohibited" attribute should not be set to any value other than 0 and 1.

# Mobile Equipment Identifier (MEID) Support

The MEID is a new attribute introduced in IS-835D that will eventually replace the ESN. It is a globally unique 56-bit identification number for a physical piece of mobile station equipment. In the interim period though, both the attributes need to be supported on the Home Agent.

The MEID NVSE will be appended by the PDSN node to the Mobile IP RRQ. When the MEID NVSE is received on the HA, and the **ip mobile cdma ha-chap send attribute A3** command is configured, the MEID value is included in the HA-CHAP access request.

CHAPTER 1

# Network Management, MIBs, and SNMP on the Home Agent

This chapter contains information pertaining to various aspects of Network Management on the Cisco Mobile Wireless Home Agent.

This chapter includes the following sections:



## Operating and Maintaining the Cisco Mobile Wireless Home Agent

This section describes configuration details, statistics, and MIBs supported by the Home Agent. A definitive description of each Mobile IP command can be found at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipras_r/1rfmobip.htm

The Home Agent can be managed using either the Cisco IOS CLI or using Cisco Works for Mobile Wireless.

Cisco's Mobile Wireless Home Agent has the following configurable parameters:

- Managing user profiles (local users)
- Configuring IP pools locally
- Configuring security associations with communicating nodes
- Configuring ingress/egress filtering
- Configuring mobile binding updates
- Configuring routing information

# Statistics

The Mobile Wireless Home Agent maintains statistics on a global basis for the following parameters:

- Advertisements, received and sent
- Registrations, requests and replies
- Registrations, accepted and denied
- Bindings
- Binding Updates
- Gratuitous and Proxy ARPs
- Route Optimization Binding Updates

The Mobile Wireless Home Agent maintains statistics on a per FA-HA tunnel basis for the following parameters:

- Source and Destination IP address of the tunnel
- Tunnel Type, IPinIP or GRE
- Reverse Tunneling allowed
- Number of Users using that tunnel
- Traffic sent on the tunnel, packets and bytes
- Traffic received on the tunnel, packets and bytes

The Mobile Wireless Home Agent maintains statistics per host, identified by NAI or home IP address, for the following parameters:

- Lifetime
- Session duration
- Traffic transmitted to the host, packets and bytes
- Traffic received from the host on the reverse tunnel, packets and bytes

**Note** The statistics can be cleared from the CLI. The MIB counters are not cleared.

## SNMP, MIBs and Network Management

The HA implements SNMPv2 as specified in the suite of protocols: RFC 1901 to RFC 1908. The Home Agent supports the MIB defined in “The Definitions of Managed Objects for IP Mobility Support UsingSMIv2,” RFC 2006, October 1995. An additional Cisco MIB, CISCO- MOBILE-IP-MIB provides enhanced management capabilities. The RADIUS MIB, as defined in RADIUS Authentication Client MIB, RFC 2618, June 1999. A full list of MIBs that are supported on the Ciscco 7200 Internet Router, Cisco 7600 Switch and Cisco 6500 Catalyst series platforms can be found at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Session counters maintained in the MIB cannot be reset using SNMP or the Cisco IOS CLI. Home Agent CPU and Memory Utilization counters are accessible using the CISCO-PROCESS-MIB.

Release 3.0 adds a Home Agent Version MIB Object.

## Conditional Debugging

The HA supports conditional debugging based on NAI, as well as conditional debugging based on the MN's home address. Only AAA and Mobile IP components will support conditional debugging.

From the CLI, it is possible to trace activity of all or a particular user identified by NAI. Monitoring the activity of a particular user, called conditional debugging, will display the user activity related to Mobile IP messages and the RADIUS messages.

This release provides an option to display the condition (username/IMSI), along with each debug statement. This helps to match a debug statement to its condition. To enable this feature, use the following command:

ip mobile home-agent debug include username

The following MobileIP debugs are supported for conditional debugging:

- debug ip mobile
- debug ip mobile host

The following AAA debugs are supported for conditional debugging:

- debug aaa authentication
- debug aaa authorization
- debug aaa accounting
- debug aaa ipc
- debug aaa attr
- debug aaa id
- debug aaa subsys

The following RADIUS debugs are supported for conditional debugging:

- debug radius
- debug radius accounting
- debug radius authentication
- debug radius retransmit
- debug radius failover
- debug radius brief

# Monitoring and Maintaining the HA

To monitor and maintain the HA, use the following commands in privileged EXEC mode:

| Command | Purpose |
|---|---|
| `Router# clear ip mobile binding` | Removes mobility bindings. |
| `Router# clear ip mobile host-counters` | Clears the mobility counters specific to each mobile station. |
| `Router#clear ip mobile secure` | Clears and retrieves remote security associations. |

| Command | Purpose |
|---|---|
| Router#**clear ip mobile traffic** | Clears IP mobile traffic counters. |
| Router# **debug ip mobile advertise** | Displays advertisement information. |
| Router# **debug aaa pod** | Displays debug information for Radius Disconnect message processing at AAA subsystem level |
| Router# **debug ip mobile** | Displays IP mobility activities. |
| Router# **debug ip mobile host** | Displays mobility event information. |
| Router# **debug ip mobile redundancy** | Displays IP mobility events. |
| Router# **debug radius** | Displays information associated with RADIUS. |
| Router#**debug tacacs** | Displays information associated with TACACS. |
| Router# **show ip mobile binding** | Displays the mobility binding table. |
| Router# **show ip mobile binding vrf** | Displays all the bindings on the HA that are VRF-enabled. |
| Router#**show ip mobile binding vrf realm** | Displays all bindings for the realm that are VRF-enabled. |
| Router#**show ip mobile globals** | Displays global information for Mobile Agents. |
| Router# **show ip mobile host** | Displays mobile station counters and information. |
| Router# **show ip mobile proxy** | Displays information about a proxy Mobile IP host. |
| Router#**show ip mobile secure** | Displays mobility security associations for Mobile IP. |
| Router#**show ip mobile traffic** | Displays Home Agent protocol counters. |
| Router#**show ip mobile tunnel** | Displays information about the mobile IP tunnel. |
| Router#**show ip mobile violation** | Displays information about security violations. |
| Router#**show ip route vrf** | Displays the routing table information corresponding to a VRF. |

APPENDIX A

# Acronyms

3GPP2—3rd Generation Partnership Project 2

AAA—Authentication, Authorization and Accounting

AH—Authentication Header

APN—Access Point Name

BG—Border Gateway

BSC—Base Station Controller

BSS—Base Station Subsystem

BTS—Base Transceiver Station

CHAP—Challenge Handshake Authentication Protocol

CoA—Care-Of Address

DSCP—Differentiated Services Code Point

DNS—Domain Name Server

ESN—Electronic Serial Number

FA—Foreign Agent

FAC—Foreign Agent Challenge (also FA-CHAP)

HA—Home Agent

HDLC—High-Level Data Link Control

HLR—Home Location Register

HSRP—Hot Standby Router Protocol

IP—Internet Protocol

IPCP—IP Control Protocol

IS835—Telecommunications Industry Association (TIA) Interim Standard for cdma2000 Wireless IP Network Standard

ISP—Internet Service Provider

ITU—International Telecommunications Union

L2_Relay—Layer Two Relay protocol (Cisco proprietary)

L2TP—Layer 2 Tunneling Protocol

LCP—Link Control Protocol

LNS—L2TP Network Server

MAC—Medium Access Control

MEID—Mobile Equipment Identifier

MIP—Mobile IP

MS—Mobile Station (= TE + MT)

MT—Mobile Termination

NAI—Network Access Identifier

NAS—Network Access Server

P-MIP—Proxy-Mobile IP

PAP—Password Authentication Protocol

PCF—Packet Control Function

PDN—Packet Data Network

PDSN—Packet Data Serving Node

PPP—Point-to-Point Protocol

PPTP—Point-to-Point Tunneling Protocol

SLA—Service Level Agreement

TE—Terminal Equipment

TID—Tunnel Identifier

VPDN—Virtual Packet Data Network